1998

Organizational innovation and redesign in the Information Age : the drug war, netwar, and other lower-end conflict

Berger, Alexander

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

ORGANIZATIONAL INNOVATION AND REDESIGN IN THE INFORMATION AGE: THE DRUG WAR, NETWAR, AND OTHER LOWER-END CONFLICT

by

Alexander Berger

March 1998

Thesis Co-Advisor	John Arquilla
Thesis Co-Advisor	Scott D. Tollefson

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
March 1998

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE
ORGANIZATIONAL INNOVATION AND REDESIGN IN THE INFORMATION AGE: THE DRUG WAR, NETWAR, AND OTHER LOWER-END CONFLICT

5. FUNDING NUMBERS

6. AUTHOR(S)
Berger, Alexander

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The end of the Cold War and the rise of the Information Age have fostered an uncertain security environment which the United States is struggling to master. The purpose of this thesis is to explore the factors that lead complex organizations to initiate large-scale structural change in the face of environmental uncertainty; and more specifically to determine how the rise of the Information Age may change the organizational requirements of the U.S. national security structure. This thesis creates a unique framework for analysis, blending principles of organization and innovation theory with the theory of information-based "netwar."

This study analyzes the organizational structures adopted by several transnational drug cartels, and compares them to that of U.S. counternarcotics forces. Next, this thesis reviews a series of recent occurrences pertaining to national security to test whether there are manifestations of netwar threats emerging, and whether new and old organizational actors are learning to adapt their structures to gain an advantage over the United States.

Finally, this thesis is both predictive and prescriptive with regard to the issues of organizational redesign. It argues that structural changes are necessary for the United States to ensure the national security in an Information Age. Then it makes recommendations that would help the U.S. security structure redesign itself to become more agile in the face of Information Age threats.

14. SUBJECT TERMS
Organizational Redesign, Innovation, Information Warfare, Drug War, Netwar, Inter-service Coordination.

15. NUMBER OF PAGES
209

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

Approved for public release; distribution is unlimited.

ORGANIZATIONAL INNOVATION AND REDESIGN IN THE INFORMATION AGE: THE DRUG WAR, NETWAR, AND OTHER LOWER-END CONFLICT

Alexander Berger, Captain, United States Air Force
B.A., University of New Hampshire, 1990
M.S., Troy State University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN NATIONAL SECURITY AFFAIRS

from the

NAVAL POSTGRADUATE SCHOOL
March 1998

ABSTRACT

The end of the Cold War and the rise of the Information Age have fostered an uncertain security environment which the United States is struggling to master. The purpose of this thesis is to explore the factors that lead complex organizations to initiate large-scale structural change in the face of environmental uncertainty; and more specifically to determine how the rise of the Information Age may change the organizational requirements of the U.S. national security structure. This thesis creates a unique framework for analysis, blending principles of organization and innovation theory with the theory of information-based "netwar."

This study analyzes the organizational structures adopted by several transnational drug cartels, and compares them to that of U.S. counternarcotics forces. Next, this thesis reviews a series of recent occurrences pertaining to national security to test whether there are manifestations of netwar threats emerging, and whether new and old organizational actors are learning to adapt their structures to gain an advantage over the United States.

Finally, this thesis is both predictive and prescriptive with regard to the issues of organizational redesign. It argues that structural changes are necessary for the United States to ensure the national security in an Information Age. Then it makes recommendations that would help the U.S. security structure redesign itself to become more agile in the face of Information Age threats.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The end of the Cold War, and the rise of the Information Age, have fostered an uncertain security environment that bears little resemblance to that of the previous fifty years. The national security structure—primarily made up of the Department of Defense, federal law enforcement, and national intelligence agencies—was designed and optimized to counter a large, single threat: the Soviet Union. Although low-intensity conflict arose, military forces and intelligence analysts focused on fighting global war and major regional conflict against the Soviets and their allies and satellites.

Along with the dissolution of the Soviet Union, dramatic advances in computer processing and telecommunications now allow for greater data storage and transfer capabilities than ever before. Global networking and connectivity allow for continuous communications and information sharing in any environment, at any time. The exponential growth of information technologies is giving the United States, and its adversaries, amazing new capabilities that may have a dramatic impact on the way war is fought.

As a result, the United States faces an uncertain security environment in which there is no single, identifiable threat to focus on. In addition to the rogue states and hostile national militaries the United States has always faced, the U.S. now confronts such ambiguous threats as transnational criminal organizations, terrorist groups, weapons proliferators and computer hackers. Many of these new threats are taking advantage of improved information technology to organize themselves as networks, with little or no centralized control and highly decentralized decision making authority. Although U.S.

national security organizations are attempting to integrate new technology into their structures, they do not appear to be adapting organizationally to meet the varied threats of the Information Age. The United States is structuring to conduct Information Operations hierarchically—with numerous organizations independently setting up separate centers, operational units, and education centers—while threats are becoming increasingly networked in structure.

The purpose of this thesis is to explore two broad questions. First, under what conditions do organizations innovate and reconfigure themselves for optimal performance? Second, and more specifically, how has the Information Age changed the organizational requirements for the U.S. national security structure? This thesis tests the theory of information-based "netwar," advanced by John Arquilla and David Ronfeldt, which states that in the Information Age organizations that take on networked structures will be more flexible, innovative, and allow a quicker decisionmaking process, making them more effective than hierarchical ones throughout the spectrum of conflict.

The first part of this thesis reviews the literature on organization theory and theories of innovation in order to investigate the relationship between environmental uncertainty and organizational structure. The Information Revolution has affected business corporations and non-profit organizations in much the same way that it is impacting the national security organizations, and there has been a significant amount of study into the causes and effects of structural change on organizational performance.

Next, the thesis focuses on a detailed case study on the structural aspects of the drug war. Illegal narcotics trafficking has been considered a threat to U.S. national security ever since the 1960's when President Nixon began the "War on Drugs." At the time, drug trafficking organizations were centrally controlled and hierarchically organized much like the law enforcement and military organizations that were established to combat them. However, in 1981 several independent drug lords met in Medellín, Colombia and agreed to pool their resources in order to combat guerrilla kidnappings of their family members. This agreement eventually expanded to include other aspects of the drug industry and led to the birth of the Colombian drug cartels, revolutionizing the way drug organizations operated. From that point on, the drug cartels took on a networked structure that has consistently outperformed U.S. interdiction and eradication efforts worldwide. The U.S. response during the drug war has been to adopt new strategies, but not a new structure.

This thesis explores today's changing security environment and proposes that the theory of netwar is becoming reality. It reviews some of the threats the United States faces in the next few years, and it compares these threats with the organizational changes being considered by the U.S. security structure to conduct Information Operations. More specifically, it shows that organizational successes and failures in past conflict can be used as "lessons learned" when preparing for conflict in the Information Age.

Finally, this thesis offers some suggestions for changes that will be necessary for the United States to counter threats from all points on the spectrum of conflict. Of the three paths the national security structure could take to prepare for the future (continuing to use the hierarchical structure, adopting a networked structure, or creating a hybrid structure with attributes of both network and hierarchical organizations) this thesis recommends the hybrid path. Although the hybrid structure does not provide the agility, flexibility, and innovation of a fully networked structure, it is the most pragmatic approach and provides vast improvements over the bureaucratic structures that exist today.

This thesis concludes with some recommendations regarding specific policies that could be enacted to foster innovation and a shift to hybrid structures. Although the list of recommendations is not comprehensive, it does provide samples of the types of changes that are required to adapt to the new security environment.

ACKNOWLEDGMENTS

I would like to thank all those who helped me in creating this thesis. I would first like to thank John Arquilla who helped lead me out of "Plato's Cave" and into the light. Without his guidance and inspiration this thesis would not have been possible. I would also like to thank Scott Tollefson for helping to spark many ideas in this thesis and giving me the latitude to investigate new areas of study. I would like to recognize two professors in the field of organization theory, Dr. Eric Jansen and Dr. Nancy Roberts, who opened my eyes to many concepts used in this thesis, and gave me a new frame with which to view our world.

I am indebted to Ambassador Rodney Minott who made it possible for me to conduct research in Washington, DC where I confirmed many of my suspicions about how policy is made. I wish to pass my thanks to all those who took the time to read drafts of this study and lend their inputs and criticisms. They include: Mr. Tom Fuhrman, Mr. Steve Stigall, Mr. Glen Davis, Col Scott Rowell, CAPT Richard O'Neill, Mr. Benson Adams, Col Diego Gantiva, LCDR Juan Imanez, LCDR Jeff Cole, and LT Paul Whitescarver. Finally, I would like to thank my wonderful wife, Samantha, who put up with stacks of research materials and many hours spent on the computer instead of going out and enjoying Monterey.

I. INTRODUCTION

> It must be considered that there is nothing more difficult to carry out, nor more doubtful of success, nor more dangerous to handle, than to initiate a new order of things. For the reformer has enemies in all those who profit by the old order, and only lukewarm defenders in all those who would profit by the new order, this lukewarmness arising partly from the incredulity of mankind, who do not truly believe in anything new until they have had actual experience of it.
>
> Niccolo Machiavelli in *The Prince*[1], 1513

A. GENERAL STATEMENT OF THE PROBLEM

We are already several years into the debate over "Information Warfare," "Information Operations," and the "Revolution in Military Affairs." Although military thinkers have been discussing the increasingly important role of technology since the mid-1970's, the realization that communications technology combined with the advances in computing power will have a revolutionary effect on the way the United States will fight wars came about in the early 1990s. Despite the overwhelming amount of debate and theorizing about operating in the Information Age, it appears that very little has been done to ensure that the U.S. will capitalize on the new opportunities presented in this dynamic time.

The end of the Cold War and the advent of the Information Age have led to a changing security environment that bears little resemblance to that of the previous fifty years. During the half-century period that the United States and the Soviet Union contested the Cold War, the forces that protect U.S. national security had to focus

[1] Niccolo Machiavelli, The Prince and The Discourses, New York: The Modern Library, 1940, 21.

principally on a single threat. The bipolar nature of the world required a large military and intelligence force that could predict and react to advances made by the enemy. Low-intensity conflict existed, but it was considered peripheral to the greater threat of global war. With the dissolution of the Soviet Union, the world now faces a multipolar environment.[2] Instead of bringing an end to conflict, the "new world order" has brought new threats from ethnic conflict and proliferation of weapons of mass destruction to transnational criminal organizations and computer hackers. The post-Cold War era has brought uncertainty to the national security environment, and it is unknown what types of military and intelligence forces will be most effective against this new kind of threat.

In addition to the end of the Cold War, the advent of the Information Age has contributed to the uncertain security environment that exists today. Dramatic advances in computer processing and telecommunications allow greater data storage and transfer capabilities than ever before. Global networking and connectivity now allows for continuous communications and information sharing in any environment at any time. The exponential growth of information technologies is giving the United States, and it's adversaries, amazing new capabilities that could have a dramatic impact on the way war is fought.

[2] The collapse of the Soviet Union, rather than leading to the United States dominating world affairs, has led to a multipolar world where global trade pacts and supranational organizations predominate. According to Robert Keohane and Joseph Nye's "theory of complex interdependence" (_Power and Interdependence: World Politics in Transition_, Boston: Little, Brown, 1977) there are multiple channels--both governmental and non-governmental, formal and informal--that connect societies. Although written prior to the breakup of the Soviet Union, this theory is even more applicable in today's internetted society.

Conflict in the new security environment is undergoing dramatic changes as well. The lines that separate war and peace have become blurred. Global conflict is no longer the most likely course of warfare, and even regional conflict between competing militaries is less likely than a decade ago. Threats come from a variety of avenues, from both nation-state and transnational organizations, with a multitude of capabilities. The traditionally hierarchical military threat is being replaced, or at least augmented, by more amorphous threats. Small groups, or even individuals, are gaining the capability to attack U.S. interests both at home and abroad.

Despite all these changes the Department of Defense, and in fact the entire national security structure, has made only marginal changes to the way it has operated since the end of the Cold War. The Chairman of the Joint Chiefs of Staff, Army Gen. John Shalikashvili, released Joint Vision 2010 which is intended to guide the military services into the 21st century. In response, each service also released its version of what their service would look like in the future. Individual services and agencies are preparing for the Information Age by creating individual Information Warfare centers and units.[3] Yet there is currently no national policy on Information Warfare, nor is there a well-developed plan to reorganize the national security establishment to match today's uncertain security environment. Procurement, training, and long-term planning continue to be based on the deliberate planning model which was created for competition in a bipolar world.

[3] The Air Force led the charge into the Information Age by creating the Air Force Information Warfare Center in 1993, the 609th Information Warfare Squadron in October 1995, and an Information Warfare Training Laboratory in November 1996. Other services and agencies have taken similar actions with the Naval Information Warfare Activity established in August 1994, the Fleet Information Warfare Center in December 1995, and the Army's Land Information Warfare Activity in mid-1996.

B. RESEARCH QUESTION

This paper seeks to answer two broad questions. First, under what conditions do organizations innovate and reconfigure themselves for optimal performance? There is a broad realm of literature studying change in large organizations that addresses the question of organizational redesign.[4] Every organization faces changes to the environment around them that require the organization to adapt and change. But large organizations have a tendency to resist change as well. This study seeks to shed some insight into what is necessary for an organization to recognize, and then react to, change.

The second question this study seeks to answer is more specific. How has the Information Age changed the organizational requirements for the U.S. national security structure? In addition to traditional military threats, the United States is now facing numerous "non-traditional" threats as a result of the end of the Cold War and the rise of new technology. Recognizing that the Information Age has presented the United States with an almost entirely new security environment, it would follow that the military and other organizations supporting national security must adapt to this new environment. This study will seek to apply lessons learned from other organizations that have faced similar types of environmental changes.

[4] In addition to some of the more popular writers on organization redesign, like Peter Drucker, this study will explore classical organization theorists including James March, Herbert Simon, and Charles Perrow, and more recent authors like Jay Galbraith and Stephen Rosen who have done empirical studies on how organizations work.

C. THEORY OF NETWAR

This study is basically testing the theory of information-based "netwar" presented by John Arquilla and David Ronfeldt ("Cyberwar is Coming!", Comparative Strategy, Volume 12, no. 2, 1993, 141-165.). Their theory states that as a result of the Information Age, organizations that take on a networked (decentralized) structures will be more effective than hierarchical (centralized) organizations. Advanced communications technology and computing power allow networked organizations to be more flexible, innovative, and permit a quicker decision making process than hierarchical organizations. This gives networked organizations an edge over hierarchical ones in conflict.

This thesis will attempt to build on "netwar theory" and offer evidence to show that this shift has indeed taken place.

D. HYPOTHESES

This study will test several hypotheses regarding conflict in the information age. Some hypotheses deal with the changing security environment, and suggest a fundamental change in the way the security establishment operates. 1) The future security environment will not be one of peace or of war, but different "degrees" of conflict. 2) The new security environment will consist of traditional military threats, but it will also include numerous threats that aren't currently dealt with by current defense structures. 3) The Information Age will be characterized by the blending of military, intelligence, and law enforcement functions and capabilities.

Other hypotheses deal specifically with organizational structure, and how organizational design influences the rate and scope of change. 4) As threats become increasingly networked, hierarchical organizations will become less and less effective when fighting them. 5) Advanced technology can be beaten by superior organizational structure. 6) Adopting a networked structure improves effectiveness against networked and hierarchical threats. 7) Decentralized control and decision making creates an environment encouraging innovation, while centralized control stifles innovation.

E. METHODOLOGY AND CASE SELECTION

Chapter II will include a review of organization theory and theories of innovation. Organizations have been faced with organizational change for centuries, and the field of organization theory has attempted to decipher some of the mystery around how organizations function. In addition to investigating the relationship between environment and organizational structure, this study will review theories regarding an organization's ability to recognize and react to change. The purpose will be to pull ideas from organization and innovation theory that may also be applicable to the military.

Chapter III will include a case study on an organization that effectively changed its structure: Western Hemisphere drug cartels. As this study is investigating causal relationships and not statistical probability, it will prove sufficient to engage in a single, detailed case study. There has been much written about the impact of the Information Age on the "high end" of the spectrum of conflict, so this study will focus on a conflict at the “low end” of the spectrum. The case study selected for this study is the drug war. In reality the drug war is neither a war, nor is it simply about drugs. The drug war exemplifies the battle between the nation-state and the transnational actor. The drug cartels are not considered a traditional threat to national security, but the product they deliver does have a harmful effect on the U.S. population and society. Unlike “traditional” military threats, transnational threats like the drug cartels are not limited by international boundaries or international law. Ambiguous threats like drug traffickers, weapons proliferators, and terrorists pose a threat to U.S. national security not because of the challenge they pose to national stability (although extreme cases like a nuclear weapon being detonated on U.S. soil could be) but because they subtly erode the confidence and faith of the American people. These transnational criminal organizations (TCOs) are examples of the widening spectrum of conflict faced by the U.S. national security structure. Although some of these threats are not new, their ability to operate outside the reach of traditional military and law enforcement organizations is increasing, partly due to their changing organizational structure.

Choosing the drug war as an example of a low-end conflict is optimal for several reasons: there is a large amount of data available, as it has been a long-term problem; the data is predominantly unclassified unlike other cases such as counterterrorism or counter-proliferation; and there is a wide range of participation, from military and government to local police and community involvement. A key reason for choosing this case is that the drug war is one of the only cases where a competing organization (the drug cartels) underwent a clear shift in organizational structure that significantly increased their flexibility and survivability. By tracking the evolution of the drug cartels as they moved from a hierarchical structure to a networked structure, it is possible to determine whether that shift made the cartel organizations more effective than the organization set up to destroy them.

In order to limit the scope of this study, it mainly focuses on the period between 1981, when President Reagan formally tasked the military with counternarcotics support, and February 1997 when President Clinton ended the "War on Drugs" by declaring it more like a "cancer" than a war. It is also during this time period that the drug trafficking organizations went from being a group of separate and competing hierarchical organizations to being a collection of cartels with a network structure that pool.resources and change relationships based on product. It will also limit its focus to drug cartels in the Western Hemisphere. Drug cartels have truly become a global phenomenon, with inter-continental alliances and trafficking routes that criss-cross the globe. However, the main interest of the U.S. national security structure, and thus the main focus of this thesis, is on the Western Hemisphere drug cartels.

Also, this study will only consider the triad of military, intelligence, and law enforcement organizations that make up the U.S. national security structure. While many other organizations, both government and non-government, are being affected by the changes of the Information Age, these very different organizations are being forced to work together to an unprecedented degree to protect the United States. Using this level of analysis, rather than just looking at the Department of Defense participation, enables the reader to see the organizational challenges of control and coordination in the ambiguous world of low-end conflict.

This study will consider four broad areas of each organization: Command and Control, Intelligence, Alliances, and Innovation. Command and control refers to the organizational structure of the institution—its formal channels of supervision and control. The basis of this thesis is to determine if the structure of the organization makes a difference in how successful the organization is in reaching its goals. Intelligence allows an organization to predict, and therefore to react to, change. Looking at an organization's capability to collect, process, and disseminate intelligence is useful in determining its ability to detect changes in its environment. Alliances are considered because the protection of national security involves multiple organizations all working, and often competing, in the same environment. Looking at an organization's relationship with other organizations is important in determining its ability to share information and resources. Finally, innovation is an organization's ability to anticipate, recognize, and react to change. It includes both operational innovation (means used to accomplish the mission in new ways) and organizational innovation (the organization's ability to institutionalize new processes, strategies or structures.)

Chapter IV will explore changes in the national security environment that have led to the current uncertain security environment. It will attempt to show that the national security environment is in fact changing, and that the United States is responding in a very predictable and out-dated way. It will review John Arquilla and David Ronfeldt's theory of netwar and review a series of occurrences pertaining to national security to predict what changes we can expect in the very near future, and then it will compare these changes with the organizational changes being suggested to conduct operations in the Information Age. More specifically, it will speculate whether organizational successes and failures in past conflict can be applied to the U.S. security structure when preparing for "Information Operations".

Chapter V will review the possibilities for organizing the national security structure to face the challenges of the Information Age. This chapter is both predictive and prescriptive with regard to issues of organizational redesign. First, it argues that there are basically three paths the U.S. national security structure can take to ensure the nation's security in the Information Age: continue operating with a hierarchical and bureaucratic structure, adopt a networked structure, or develop a hybrid structure. Then, it will offer some suggestions for changes that will be necessary for the United States to counter threats from all points on the spectrum of conflict.

II. ORGANIZATION THEORY

A. REVIEW OF ORGANIZATION THEORY

> The intellectual and organizational changes necessary to evaluate new ways of fighting are as important as the development and production of new technologies.
>
> Stephen P. Rosen, Winning the Next War[1]

> Over the past decade, the American commercial sector has reorganized, restructured, and adopted revolutionary new business and management practices in order to ensure its competitive edge in the rapidly changing global marketplace. It has worked. Now the Department must adopt and adapt the lessons of the private sector if our armed forces are to maintain their competitive edge in the rapidly changing global security arena.
>
> Secretary of Defense William Cohen[2]

1. Definition of Terms

Before reviewing the literature on organization theory, it is useful first to define some common terms. Webster's Dictionary defines an organization as "an association or society of people working together to some end." Organization theory refers to the broad body of literature that explores the structure and design of organizations. Organization theory can be broken down into sub-specialties, looking at different aspects of the organization. Some organization theorists look at an organization's structure, and suggest ways an organization can redesign itself for better performance. Other organization

[1] Stephen P. Rosen, Winning the Next War: Innovation and the Modern Military, Ithaca, NY: Cornell University Press, 1991, 128.

[2] From the final report of the 1997 Quadrennial Defense Review.

theorists look at an organization's processes or personnel, while others explore the importance of rewards systems used to motivate employees. Organization theorists both describe how organizations operate, and suggest how they can improve to operate more effectively and efficiently.

An organization's "structure" directs how tasks are allocated, who reports to whom, and how formal coordination and interaction takes place. "Organization design" looks at an organization's structure and tries to determine how constructing and changing organizational structures can improve operations to meet goals more efficiently and effectively.

An organization's "environment" refers to the world that exists outside the organization. It often denotes the industry or market of a particular organization, but it is not limited to an organization's immediate surroundings. "Environmental uncertainty" results when the environment changes so rapidly that an organization can not keep up through changes of its own. In response, the organization is forced to decrease environmental uncertainty or adapt to the new environment.

"Organizational learning," also known as innovation, is an organization's ability to recognize and adapt to the changing environment. An organization's "culture" is the shared values, beliefs, expectations, and norms of the organization.

2. Why Use Organization Theory?

Some may question the utility of using organization theory, mainly used by the business world, to explain how the U.S. military, intelligence services, and law enforcement agencies can operate more efficiently. Many argue that the defense establishment is not a corporate business; their mission is to use force to protect the vital interests of the United States. Protecting national security involves the risk, and sometimes sacrifice, of human lives. There is no "profit margin" in protecting the nation.

This thinking, however, is too narrow for today's rapidly changing environment. Organization theory applies to any type of organization, whether it be a Fortune 500 company, a non-profit hospital, or the national security structure. Organization theory simply investigates relationships between strategy, structure, processes, people and rewards. It helps to determine the most efficient mix of these five components. It is true that most research on organization theory has been done in the corporate realm, but much literature exists applying organization theory to all sorts of organizations including the military. Looking at the various services' plans for operating in the 21st century shows that the military intends to move toward a period of organizational change that has previously been seen only in the business world.

There is another reason that using organization theory is important. Organizational theorists use the term "frames" to describe the different ways one can look at problems. Frames are the filters that each of us use to look at the world. Our frames can be influenced by biases, past experiences, cultures and any other number of factors. It is important to realize, though, that the frames that we look through may be very different than the frames that influence others' decisions. According to organization theorists, frames also act as lenses to help us see our environment better. Like a telescope, the more lenses we have the better we can see. Consequently, the more frames one has to look at the world, the better he will be able to understand what he sees. We can learn to see through new frames, and it is beneficial to have many different points of view when dealing with new challenges. In the military's recent Total Quality Management movement[3] it is called "adding a new tool to your toolkit," "shifting paradigms," or "thinking out of the box". However, what many do not realize is that one cannot view the world through a frame one does not understand; and one cannot think out of the box unless one has another box in which to step. Organization theory simply provides another frame with which to look at the changing national security environment, and the changes made by the U.S. security structure.

Of the four main frames organization theorists look at—the structural frame, the human resource frame, the political frame, and the symbolic frame—this paper will discuss the structural frame. How will an organization react when problems arise and the structure no longer fits the situation? The structural perspective is only one way of looking at the security organization, but it has long been assumed that the military and government will always operate hierarchically and the structural debate has gone unexplored. Even more important, however, is that it appears the Information Age has brought with it threat organizations that are using new organizational structures to counter the United States' superior numbers and equipment. With this in mind, investigating the structural aspects of these organizations is most relevant to this thesis.

[3] Refers to the Defense Department's emphasis on feedback and continuous improvement based on the teachings of Edward Deming.

Finally, in the past decade the corporate world has been shaken by the same Information Revolution that is affecting the national security structure. Due to the competitive nature of the business world, where organizations either change or go bankrupt, these organizations have been much more responsive to recent environmental changes than the security structure has. Many organization theorists believe that mastering organizational redesign will be the basis for gaining a competitive advantage in the future.[4] In other words, those organizations that best learn to adapt their structures and strategies to environmental changes will be the ones to succeed. Therefore, it is beneficial to look at organization theory to see what security organizations can learn from the successes and failures of business corporations.

3. A Brief History of Organization Theory

Organization theory, in some form or another, has been around for thousands of years.[5] Socrates wrote of the need to establish schools of management. Plato recognized the need for specialization, and two millennia later Adam Smith applied the concept of specialization to manufacturing. However, the modern field of organization theory first emerged with the German social scientist Max Weber at the beginning of the 1900's and his investigation of authority relations inside an organization.[6] Weber sought to understand why individuals obeyed the commands of other individuals. Weber identified

[4] Jay Galbraith and Edward Lawler III, "Challenges to the Established Order," in Organizing for the Future, San Francisco: Jossey-Bass Publishers, 1993, 2.

[5] An Egyptian manuscript dated from 4000 B.C. outlines a father's advice to his son who is about to start his own business. He tells his son of the importance of long-term planning, and organizing and controlling his employees. (Pradip N. Khandwalla, The Design of Organizations, New York: Harcourt Brace Jovanovich, Inc. 1977, 132.)

[6] Khandwalla, 1977, 133.

three “ideal types” of legitimate authority. He found that authority is achieved by the personal qualities of a leader (“charisma”), due to inherited status (“traditional”), or from legal recognition of authority (“rational”).[7]

Focusing on the rational model, Weber developed a theory about what would be the “ideal” organizational structure in terms of efficiency. What he came up with was the “bureaucracy”. Although we now recognize the bureaucracy as the traditional organizational structure for businesses, schools, hospitals, and governments, at the time it was largely a hypothetical model of the ideal organization.

Weber proposed several characteristics of bureaucracy that, unlike the modern idea of inefficient bureaucracy, would lead to an organization’s peak performance. First, an organization should have a clear *division of labor*, with jobs broken down into simple, routine, and well-defined tasks. Second, there should be a *well-defined authority hierarchy* with multiple levels and vertical delineation of responsibility. Third, there should be *high formalization*, using formal rules and procedures to ensure uniformity and regulate behavior. Fourth, the *impersonal nature* of the organization should ensure controls are applied uniformly throughout the organization. Fifth, employment decisions (selection and promotion) should be *based on merit and performance* rather than favoritism or nepotism. Sixth, the organization should have *career tracks for employees*,

[7] Max Weber, The Theory of Social and Economic Organization, trans. A. M. Henderson and Talcott Parsons, ed. Talcott Parsons, New York: Free Press, 1947, 328.

exchanging job tenure for career commitment. Seventh, there should be a *distinct separation of members' organizational and personal lives.*[8]

According to Weber, the strength of the bureaucracy is that, like a machine, each part of the system works toward maximizing the organization's goal. "Precision, speed, unambiguity, knowledge of the files, continuity, discretion, unity, strict subordination, reduction of friction and of material and personal costs—these are raised to the optimum point in the strictly bureaucratic administration...."[9]

Beginning in the 1950's, a new group of organization theorists from Carnegie-Mellon University (known as the Carnegie School) began to focus on understanding decision-making in organizations. James March, Herbert Simon, Richard Cyert, and others have done various studies on how organizational decisions are made, and how they can be made more effectively.

In 1958, March and Simon co-authored a book entitled Organizations[10] to fill the gap in studies of formal organizations. Their book, one of the first studies dedicated specifically to figuring out how organizations work, seeks to test various theories of organizations taken from other academic fields. March and Simon focus on the human side of organizations, showing that theoretical models of how organizations are supposed to work are often inaccurate because they do not take into consideration the limitations of human decision makers. In addition to being limited by time and attention, decision

[8] Stephen P. Robbins, Organization Theory: Structure, Design, and Applications, 3d. ed., Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1990, 233.
[9] Max Weber, From Max Weber: Essays in Sociology, trans. and ed. Hans Gerth and C. Wright Mills, Oxford, UK: Oxford University Press, Inc., 1946.
[10] James March and Herbert Simon, Organizations, New York: John Wiley & Sons, Inc., 1958.

makers are limited in their mental capacity to handle multiple problems. Additionally, external factors such as office politics and other's preferences can effect the decisions made. Rather than being rational and thorough in their decision making process, decision makers often "satisfice" (a combination of satisfy and suffice) or make the easiest decision that will solve a problem.[11]

This theme is continued in March and Cyert's A Behavioral Theory of the Firm[12] in which they investigate how business organizations make economic decisions. In this book, they write about the coalition-building effect of organizations. Decisions are not made in a vacuum, independent of other decisions and inputs. Rather, decisions are made through negotiation and bargaining. One of the goals of an organization is to avoid uncertainty, especially long-term uncertainty. Because long-term forecasting is so difficult, decision makers often operate with short-term interests in mind. This approach prevents an organization from searching for new alternatives to existing or future problems.[13]

This eventually led to March and Johan Olsen's "garbage can model of organizational choice."[14] March and Olsen theorized that problems and solutions are grouped into various "garbage cans" that denote an organization's areas of knowledge. Problems that arise in the organization are thrown into a garbage can where it awaits a

[11] Herbert Simon, Models of Bounded Rationality, Cambridge, Mass: MIT Press, 1982,

[12] Richard Cyert and James March, A Behavioral Theory of the Firm, Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1963.

[13] Derek Pugh and David Hickson, Writers on Organizations, Newbury Park, CA: SAGE Publications, 1989, 143.

[14] James March and Johan Olsen, Ambiguity and Choice in Organizations, Bergen, Norway: Universitetsforlaget, 1979.

solution. Solutions are presented by previous experience or ideas by participants in the decision making process. According to their garbage can model, if a problem arises that has no known solution it is ignored or tossed into a garbage can to await a solution. For example, if an organization is presented with a new problem (change in environment) it seeks a solution within the organization. If someone in the organization has dealt with a similar challenge before, he is given the task of fixing the problem. However, if no one in the organization has a solution for the problem, it is left unsolved or "fixed" using an inappropriate solution. According to the garbage can model, an organization is a solution looking for problems. In other words, an organization will seek to solve the problems it is most comfortable solving using the particular experience of its members.[15]

Around the same time, Charles Perrow was also studying the workings of organizations. In his 1972 book Complex Organizations: A Critical Essay,[16] Perrow seeks to criticize several commonly accepted theories of organization theory and present his own model, built on Weber's writings on bureaucracy and March and Simon's Organizations. Rather than looking at the frailties of human behavior, Perrow looks at the structure of organizations. He finds that the bureaucracy can be a viable and desirable form of organization, despite criticism from the human relations and other schools of organization theory. However, he points out that bureaucracies are only optimal when "the tasks people perform are well understood, predictable, routine, and repetitive..."[17]

[15] Pugh and Hickson, 1989, 145.
[16] Charles Perrow, Complex Organizations: A Critical Essay, Glenview, Ill.: Scott, Foresman, and Co., 1972.
[17] Ibid., 166.

Otherwise, he says, some other form of organizational structure, one that is more decentralized and interactive, is necessary.

More recently, organization theory has expanded in scope and has become popularized. The field of organization theory has become increasingly diversified, and numerous sub-specialties have emerged to focus on different aspects of operations. Authors such as Peter Drucker, John Naisbitt, and Alvin Toffler have written best-selling books on organizational change and the nature of the changing business environment. Rather than just limiting itself to trade journals, articles on management and organizational redesign can be found in all types of magazines and newspapers. The study of new management techniques has spread to virtually all types of organization, including profit and non-profit organizations. The application of organization theory to businesses and government has created an entire industry for those who understand and can assist in organizational redesign.

For decades it was accepted that the bureaucracy was the optimal organizational form for corporations and governments. Oliver Williamson, in his 1975 book Markets and Hierarchies,[18] investigated the costs and benefits of hierarchical organizations versus unstructured markets. He determined that the hierarchy was an organizational form that improved on the market forces, which were inefficient and unorganized. He showed that hierarchies can help an organization improve productivity by providing specialization and commonality. But Williamson also showed that there is a point where hierarchies are no

[18] Oliver Williamson, Markets and Hierarchies: Analysis and Antitrust Implications, New York: Free Press, 1975.

longer beneficial because the higher levels of the hierarchy lose touch with the lower levels and the organization loses its common purpose. In later works, Williamson advocates the use of "hybrid" organizational forms—inter-firm networks that strike a balance between the properties of hierarchical organizations and those of markets.[19]

With the Information Age came global connectivity and increased environmental uncertainty, and there has been an increased interest in organizational redesign. Many organization theorists are now calling for a shift towards networked organizations; organizations that are more decentralized in decision making and flatter in structure.

The remainder of this chapter will investigate what impact environmental uncertainty has on an organization, what options it has to deal with uncertainty, and how an organization can radically change its organizational structure to fit a new environment.

4. Rational-Systems Model

One approach to organization theory, called the "rational-systems model", focuses on the goals, roles, and technology of the organization and attempts to find the best structure to fit the organization's purpose and environment.[20] As stated earlier, organization theory helps an organization find the right mix of strategy, structure, processes, people and rewards in order to reach its goals in a given environment. The rational-systems theory states that all five of these concepts are interrelated, and changes in any one means evaluating, and possibly adjusting, the others. If an organization's

[19] Anna Grandori, and Guiseppe Soda, "Inter-firm Networks: Antecedents, Mechanisms, and Forms," Organization Studies, 16/2, 1995, 183-214.

[20] Lee Bolman and Terrence Deal, Reframing Organizations, San Francisco: Jossey-Bass Publishers, 1991, 9.

strategy or mission changes, the organization will likely be forced to change its processes and possibly its structure. If the structure and processes change, it may require people to be hired, trained, or rewarded differently. None of these components exist in a vacuum. When depicted pictorially, the relationship between these five components takes on a star-like shape as seen in Figure 2.1.

This model, called the "Star Model", helps us see that changes in one part can affect the entire system. Additionally, surrounding the entire organization, and in many ways holding it together, is the organizations' culture. External to the organization, environmental factors are constantly bombarding the organization with new challenges. These environmental factors, when the organization has no prior experience dealing with them, leads to environmental uncertainty.

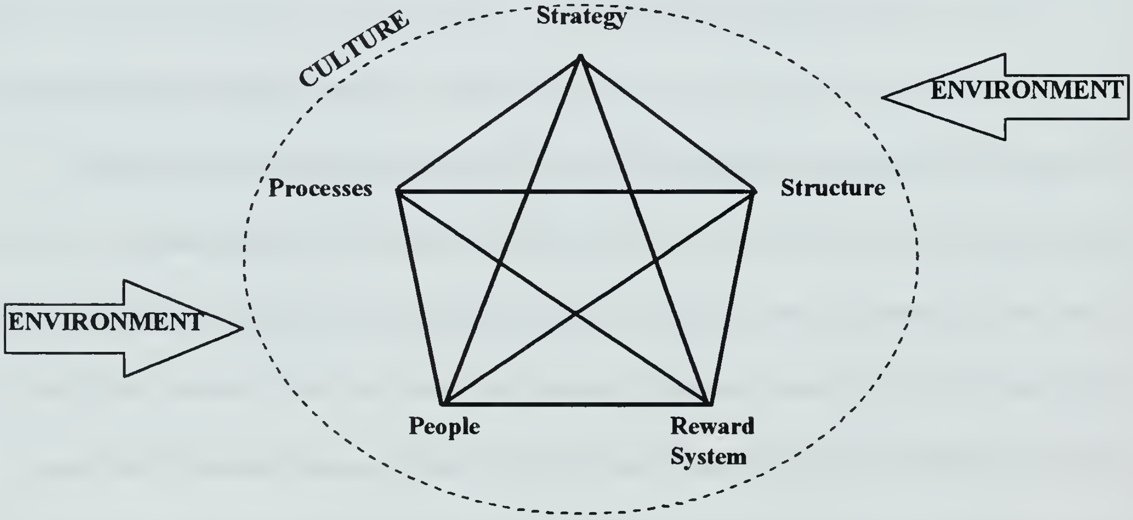

Figure 2.1. The Star Model

5. Dealing With Uncertainty

There are two main types of uncertainty that effect an organization: task uncertainty and environmental uncertainty. Task uncertainty deals with the variation in the way a worker does in his job. For example, a fry cook at a fast food restaurant has very little task uncertainty because he makes fries exactly the same every time, while a corporate executive has high task uncertainty because he is forced to deal with a wide variety of situations. Some areas of the military have low task uncertainty, such as artillery gunners who have the same procedure every time they shoot their gun. Others, like fighter pilots, have higher task uncertainty because of constantly changing equipment or tactics.

Environmental uncertainty refers to change in an organizations surroundings. For some organizations, like salt manufacturing, there is low environmental uncertainty because suppliers, product lines, and even competition remain mostly static. The computer industry has very high environmental uncertainty because of technological advances and constantly evolving competition. For the military, uncertainty can be very high on the battlefield. In fact, a key goal of warfare is to increase the environmental uncertainty of one's adversary while decreasing one's own environmental uncertainty. At the same time—especially during the Cold War—environmental uncertainty has traditionally been low at the strategic level.

According to Jay Galbraith, uncertainty is "the difference between the amount of information required to perform the task and the amount of information already possessed by the organization."[21] With this definition in mind, he says there are several ways in which an organization can decrease uncertainty—the goal of every organization. The traditional means a hierarchy uses to reduce uncertainty is to impose rules and controls (decisions made in advance of their implementation), to set goals that the organization must meet (minimum and maximum targets for productivity), and to establish a hierarchy of authority (passing on problems to higher, more experienced managers). But as an organization encounters dramatically new environments, rules and goals are no longer effective as guidance. Workers are unsure of how to proceed and must request guidance from higher levels of authority. The top levels of management receive these requests for guidance and pass information back down to the workers. Galbraith proposes, "the greater the task uncertainty, the greater the amount of information that must be processed among decision makers during task execution in order to achieve a given level of performance."[22] When uncertainty becomes too great, decision makers are unable to process information quickly enough to keep up with the demand, and organizational performance is impaired.

According to Galbraith, there are five ways to deal with uncertainty. First, an organization can reduce uncertainty by modifying its environment. The goal is to return the operating environment to its original state and reduce the need for information processing. Second, an organization can reduce its level of performance, expecting less out of the organization thus producing "slack resources". This reduces the amount of

[21] Jay Galbraith, Organization Design, Menlo Park, CA: Addison-Wesley Publishing Co., 1977, 36.
[22] Ibid., 36.

information that has to be processed in a set period of time and prevents overloading the channels of communication. Third, an organization can create self-contained tasks so that each unit has all the resources it needs to accomplish a specific part of the overall task. This also reduces the amount of information exchanged as each unit operates independent of the others.

The fourth way to reduce uncertainty is to improve the organization's vertical information systems, such as advanced computers or telecommunications. This allows more information to be sent to the right people more quickly, preventing an overload in the system. Finally, an organization can reduce uncertainty by creating lateral relations, also known as decentralization. This increases the organization's capacity to process information by pushing the decision making process down to where the information is available and allowing for information sharing across lines of authority.

An organization faced with uncertainty must select which of these five methods it will employ in order to reduce uncertainty and remain competitive. If an organization ignores the problems emerging from uncertainty, reduced performance (option two) will automatically occur. According to Galbraith, "[t]he task information requirements and the capacity of the organization to process information are always matched. If the organization does not consciously match them, reduced performance through budget overruns, schedule overruns, etc. will occur in order to bring about equality."[23]

[23] Ibid., 55.

Applying Galbraith's theory on reducing uncertainty to today's national security environment can be useful in helping to decide how the national security structure should deal with today's changing security environment. The first three options, manipulating the environment, and reducing information flow through creation of slack resources and self-contained task units are unlikely choices. First, the national security environment that resulted from the end of the Cold War and the rise of the Information Age is not likely changeable. Also, because of the vast increases in information communication and processing, it is unlikely that the security establishment would choose to decrease the flow of information. Therefore, the security structure is left with two options, investment in vertical information systems and creation of lateral relations.

Current military and security thinkers are touting the improvements in telecommunications and information processing possible in the Information Age. Admiral Owens' "system of systems" advocates the application of telecommunications technology to all levels of command so that everyone is operating with the same information. He is, in effect, advocating investment in vertical information systems. However, it is not clear that his vision also includes the horizontal integration of information. Supporters of the "system of systems" envision integrating information from a variety of sources, and permitting increased guidance from senior leadership who have greater "topsight". This increases the amount of information that flows vertically, but it does not necessarily allow for decentralizing decision making or create lateral relations.

The question, then, is: does improving vertical information systems give enough information-processing capability to deal with the level of uncertainty that exists now and in the future? Given that the national security structure is facing a wide variety of threats, some of which cannot even be quickly detected or identified, is environmental uncertainty greater than even the national security establishment of the future can deal with? There are two clues that indicate simply investing in vertical information systems will not be enough. First, the "system of systems" deals solely with military and intelligence organizations. At present, no one is talking about integrating law enforcement agencies into the future force structure. There may be good reasons for this, like the Posse Comitatus law which, generally, prohibits the military from being used to do law enforcement. However, the "system of systems" is being advocated as a new warfighting tool and not as a new tool to protect national security at home. Second, the force structures being adopted by the "low-end" threats like transnational criminal organizations and terrorist groups incorporate vertical information processing and lateral relations. The very same information technology that is being advocated by the military for the "system of systems" is available to competing organizations. Yet at the same time, these groups are using improved lateral relations to make information flow even quicker.

6. Organizational Structure

So far we have seen how changes in information processing capability can help an organization reduce uncertainty without changing its organizational structure. Although the fifth option, creating lateral relations, somewhat changes the relationship from vertical to horizontal, the hierarchical structure still dominates. However, organization redesign can also be used to reduce uncertainty and improve communications flow throughout an organization. Changing an organization's structure affects the way in which the organization operates during times of calm and crisis. Different organizational structures have different attributes that, depending on the environment, make an organization more or less efficient.

Although organization theorists have come up with a variety of names and descriptions for the different forms of organization, there are basically six different organizational structures that range from the traditional bureaucracy to a true network.[24] It is important to note that these six organizational forms are not distinctly different from each other, but represent different points on a structural continuum that becomes increasingly decentralized. The following section provides a brief overview of the six structures, and some of their strengths and weaknesses.

[24] Gareth Morgan, Creative Organization Theory: A Resourcebook, Newbury Park, CA: SAGE Publications, 1989.

a. *Rigid Bureaucracy*

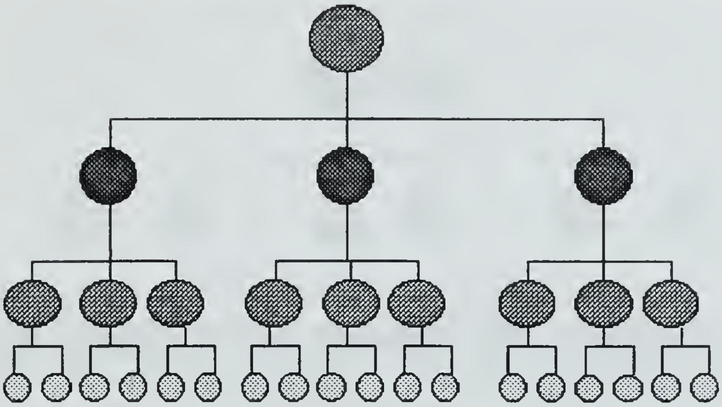

Figure 2.2. The Rigid Bureaucracy
(Gareth Morgan, Creative Organization Theory, 1989, p. 66)

The "rigid bureaucracy" is what one traditionally thinks of when hearing the word "bureaucracy". The command structure is completely hierarchical, with decisions being made at the top and each level of command reporting to level above it. The organization uses rules, regulations, and standard operating procedures that gives direction on all significant operational processes, and diversion from the norm is not tolerated. Very little coordination is required because almost every contingency is understood by everyone. However, middle managers ensure that each part of the machine is completing its assigned task. This organization is the most efficient organizational form when operating in an extremely stable environment with virtually no environmental uncertainty.

b. *Bureaucracy With a Senior "Management" Team*

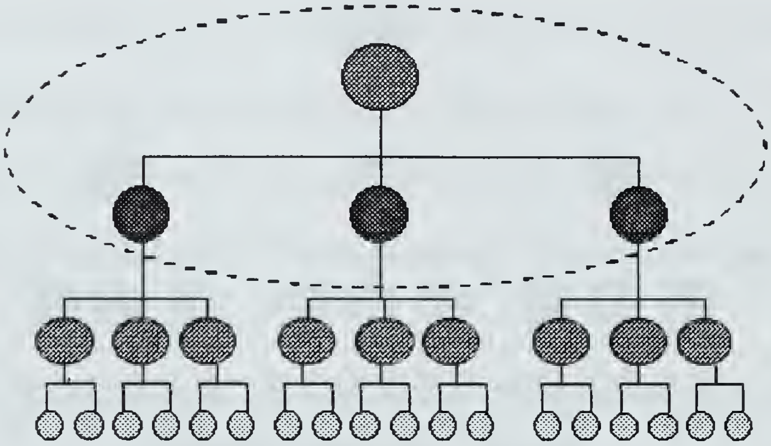

Figure 2.3. The Bureaucracy with a Senior "Management" Team

(Gareth Morgan, Creative Organization Theory, 1989, p. 66)

This organization is still bureaucratic, maintaining numerous levels of vertical command. However, in this case the top manager has a "management team" to help him deal with a variety of problems that emerge. The management team—made up of senior leaders and department heads—meets periodically to make policy decisions and discuss problems that can't be dealt with through the organization's existing processes. Each department head has authority over their area of specialty. This type of organization results when a changing environment presents the organization with new situations for which it has not previously planned.

c. *Bureaucracy With Project Teams and Task Forces*

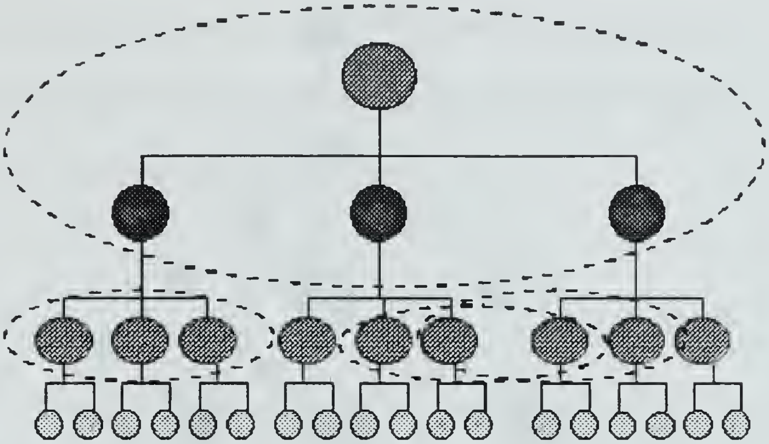

Figure 2.4. The Bureaucracy with Project Teams and Task Forces

(Gareth Morgan, Creative Organization Theory, 1989, p. 66)

This organizational form exists when senior management cannot solve all the problems that require interdepartmental coordination. The organization creates temporary project teams or task forces that include lower level members of the organization. Although it appears that decision making has been decentralized in this organization, the sense of organizational hierarchy is still strong. Members of the project team or task force remain loyal to their department (where promotions and rewards lie) rather than to the team. Conflict results when each member maintains his "departmental line" and decisions are made through negotiation and bargaining rather than what's best for the organization. Difficult decisions are passed on to the senior management team for resolution.

d. *The Matrix Organization*

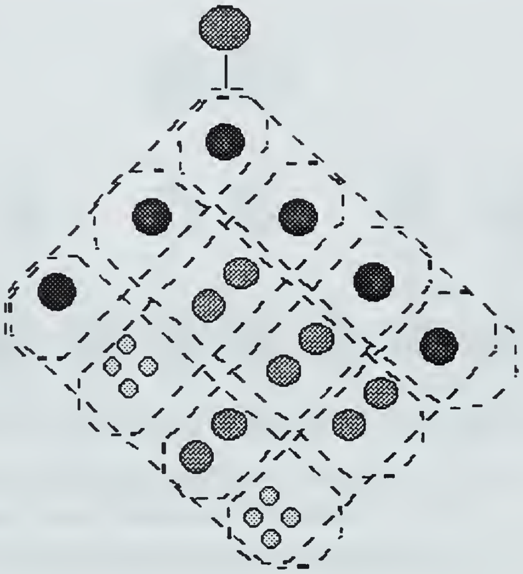

Figure 2.5. The Matrix Organization
(Gareth Morgan, Creative Organization Theory, 1989, p. 66)

The "matrix" organization, sometimes called a "mirror-image" structure,[25] results when the organization decides to give equal attention to functional departments (production, sales, marketing, administration, etc.) and various business or product areas. Although employing some vertical specialization, the organization also encourages lateral communications between similar processes. For example, an aircraft manufacturer will have a research and development office, a production branch, purchasing specialists, and a quality-assurance staff that are vertically organized. But a matrix organization will also have product managers who follow their particular part of the aircraft (wing, fuselage, cockpit) through the entire development, acquisition, and production process. Each

[25] Jay Galbraith, "The Business Unit of the Future," in Organizing for the Future, San Francisco: Jossey-Bass Publishers, 1993, 48.

member of the functional departments must focus on a variety of products, while members of the product teams must understand all parts of the manufacturing process. This form of organization provides flexibility and deals well with environmental uncertainty.

e. *The Project Organization*

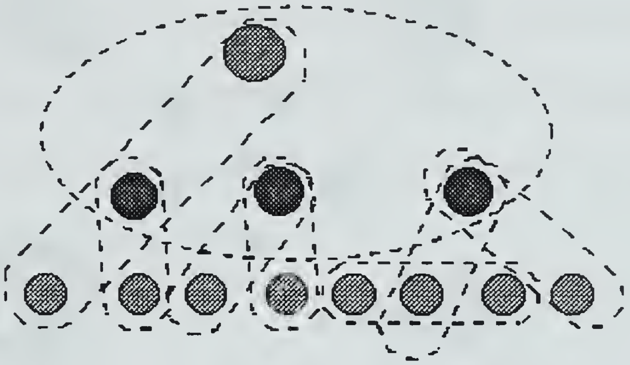

Figure 2.6. The Project Organization

(Gareth Morgan, Creative Organization Theory, 1989, p. 66)

Like the matrix organization, the project organization relies on project teams to perform its major processes. This organization relies even less on functional departments, which exist primarily to support the project teams. Teams contain specialists who coordinate efforts, but encourage innovation and creativity within the bounds set by the senior leadership. Senior leadership exists mainly to give strategic direction to the organization, while the teams use whatever means practical to achieve their goals. There is little formal coordination, and there is a regular exchange of information throughout all levels and areas of the organization. The organization places an emphasis on educating members about the nature of the organization and its mission, which in turn guides and motivates members. This organization values innovation, and its flexibility enables it to operate efficiently in a highly uncertain environment.

f. *The Organic Network*

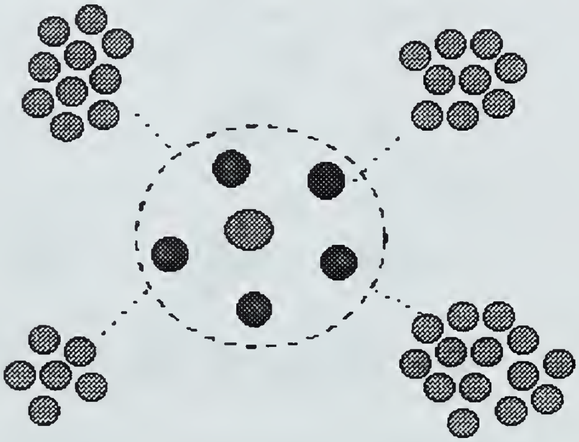

Figure 2.7. The Organic Network
(Gareth Morgan, Creative Organization Theory, 1989, p. 66)

This organization has taken on the form of a loosely coupled network. It does not maintain a large staff of workers, but rather subcontracts other organizations or individuals to perform the key processes. The organization has a small cadre of staff who provide a strategic direction and provide operational support to maintain the network. The network of organizations provides the meat for the bones provided by the central staff. An example of this would be an organization in the fashion industry that creates a name and image but then contracts out product design, production, and distribution of the apparel. From an outside perspective, the organization has a clear identity. But in reality, it is just a network of firms brought together by the core, organized around a specific product. Products change based on the latest, or even future, trends. The network is really a "system of firms" that lack a clear structure or a differentiation between supplier and organization member. The network organization is the most efficient organizational form when operating in an extremely unstable environment with a high degree of environmental uncertainty. It allows the main part of the organization to focus on its core competencies while allowing other organizations and entities to provide what they do best.

The organic network model pictured in Figure 2.7 represents the "star" or "hub" configuration. There are other forms of network structures that provide greater or lesser connectivity, as shown in Figure 2.8.

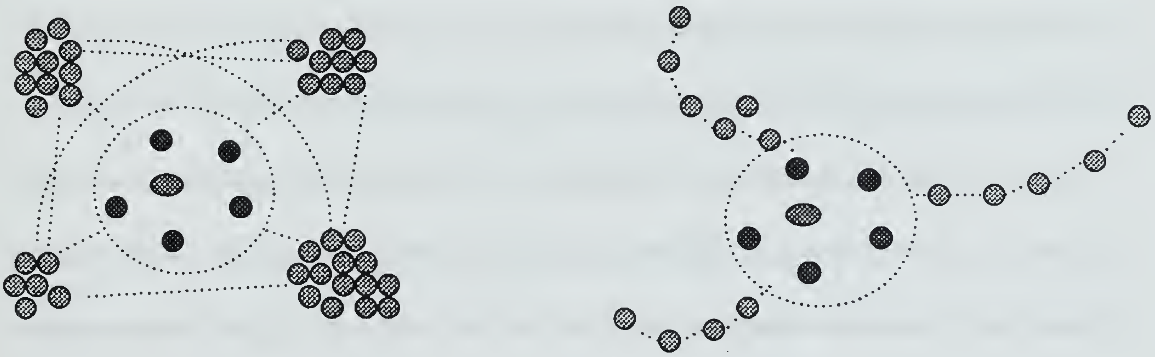

Figure 2.8. All-Channel and Chain Network Structures
(John Arquilla and David Ronfeldt, The Advent of Netwar, 1996, p. 49.)

The difference between the "star," "all-channel," and "chain" configurations is the level of interconnectedness between different nodes or parts of the organization. The all-channel configuration utilizes the greatest amount of connection between nodes, with free flowing communications throughout all parts of the organization. The star configuration is distinguished by free flowing communications between different collections of nodes (centered around a particular process or product), but inter-group communications are channeled through the central core. With the chain configuration, information is channeled through sequential nodes and communications are limited. Each configuration has certain applications, and a network organization can choose the one that is most applicable or it can create a hybrid using different configurations for different tasks.[26]

In the past, the large amount of communications required to support the network design limited its usefulness. Because the centralized nature of the bureaucracy limits communication requirements, hierarchies have traditionally been the most efficient means of structuring an organization. However, recent advances in information technology have enabled the network structure to show its full potential, allowing rapid decision making and adaptiveness while gaining efficiency in its operations.

The key to a network's effectiveness is the "network integrator," the focal company or node which brings together separate functions and companies. While other parts of the network are essential to the operation, the network integrator is the part that performs the dominant function. Using the fashion industry as an example, even though the brand-name organization may not produce or distribute the clothing, it controls the network because it has an already-established name. The manufacturers who make the clothing could try to branch off on their own, but they would probably not do as well under their own name as they would under the brand-name.

Of the six structures described above, the first three are largely hierarchical in nature. Although the project teams and task forces in the third model encourage cross-

[26] In The Advent of Netwar (John Arquilla and David Ronfeldt, Santa Monica, CA: RAND, 1996.) Arquilla and Ronfeldt use the example of a netwar actor that uses an all-channel structure for its core, but utilizes star or chain structures for tactical operations.

functional communications, teams are temporary and the basic structure is highly bureaucratic. The last three structures abandon the vertically organized hierarchy for an organizational structure that formalizes lateral integration. When organization theorists describe the organization of the future, they describe organizations that are flatter, more lateral, and less hierarchical.[27]

It is important to note that it is possible, and in many cases desirable, to move along the continuum and adopt new organizational forms to fit a given environment. Aside from being able to shift organizational structure to move along the structural continuum, it is also possible to create an organization that has attributes of several organizational forms. An organization may include a mix of several organizational structures depending on the needs of the organization. Many businesses use a "hybrid" structure using a traditional bureaucracy for processes that need to be consistent while using a network-type organization for product design or customer service.[28] Although organizations can also move along the continuum, it is unlikely that any organization will move from one end of the spectrum to the other without encountering severe resistance and involving significant resources for training and education. A shift from one end of the spectrum to the other would be truly revolutionary, and involves cultural as well as structural changes. But from a systems point-of-view, adapting an organization's

[27] Jay Galbraith, Edward Lawler III, and Associates, Organizing for the Future, San Francisco: Jossey-Bass Publishers, 1993.

[28] According to The Boundaryless Organization (Ron Ashkenas et al., San Francisco: Jossey-Bass Publishers, 1995), one of the largest private label credit card providers, Retailer Financial Services (RFS), organized around key processes using a centralized model for highly consistent processes (financial reporting, credit scoring, telecommunications, etc.) and a decentralized structure for processes that supported customers.

structure to fit its environment is highly advantageous. Table 2.1 helps show which types of organizations are optimal for different types of environments.

		Simple	Complex
CHANGE	Dynamic	3. Moderately high perceived uncertainty Environment: Small number of components; these components are somewhat similar to one another, and they are in a continual process of change. Structure: Low complexity, low formalization, and centralization.	4. High perceived uncertainty Environment: Large number of components in the environment; these components are not similar to one another, and they are in a continual process of change. Structure: Low complexity, low formalization, and decentralization.
	Static	1. Low perceived uncertainty Environment: Small number of components in the environment; these components are somewhat similar to one another, remain basically the same, and are not changing. Structure: High complexity, high formalization, and centralization.	2. Moderately low perceived uncertainty Environment: Large number of components in the environment; these components are not similar to one another but remain basically the same. Structure: High complexity, high formalization, and decentralization.
		COMPLEXITY	

Table 2.1. Environmental Complexity and Change
(Stephen P. Robbins, Organization Theory: Structure, Design, and Applications, 1990, 160.)

For the past fifty years the United States has faced a relatively simple and static environment. There was one major threat—that of the Soviet Union—and other conflict was generally a subset of this greater struggle. The fight against communism gave the U.S. security structure a common enemy on which it could focus its efforts, and change was slow and predictable. The national security structure established to counter the Soviet threat was strictly hierarchical, with high formalization of roles and a centralized command structure. During the Cold War, the U.S. security structure matched the security environment that existed.

Today's national security environment is dramatically different. As will be shown in later chapters, the global security environment has become increasingly dynamic and complex. In addition to a greater number of threats in the world, the new threats have a variety of goals and methods, and they are continually changing. The purpose of this thesis is to determine if the United States is adapting its structure to meet this new environment.

With the understanding that there are several different types of organizational forms, and the knowledge that some structural forms are more effective than others depending on the environment, one might ask how an organization recognizes the need to change. An organization that recognizes and adapts to environmental changes is described as being innovative. Therefore, innovation will be the focus of the next section.

B. INNOVATION THEORY

Webster's Dictionary defines innovation as the act of introducing something new. Organization theorists call this invention, believing innovation is the process of developing the invention so it can be put to practical use. Although many equate innovation to the production of a new product or service, innovation can also include improving a process, an organization's structure, management style, or method of problem solving.[29]

The study of innovation is almost as broad as the field of organizational theory. Innovation theorists study different levels of analysis, from networks of organizations and societies all the way down to individual innovation. For the same reasons that this thesis is focused on the structural frame of organization theory, it will focus mainly on organizational innovation that effects the structure of the organization rather than on individual innovation. It must be pointed out, however, that there is a correlation between individual innovation and organizational innovation. History shows individual innovation will likely fail unless the organization is open to new ideas and able to incorporate the innovation into its everyday operations. However, an organization that stifles individual innovation will encounter more difficulty when trying to change its structure.

As the Revolution in Military Affairs is effecting the military, so is the Revolution in Business Affairs changing the way businesses operate. In the competitive world of business, corporations must constantly evaluate their processes, strategies, and structures in order to remain ahead of others in their field. Traditionally the military only gets to test its effectiveness during wartime, when the full measure of weapons and strategies can be exercised. Businesses, on the other hand, are constantly evaluating their effectiveness which is usually measured in profit and productivity. Therefore, it is beneficial to review

[29] Pradip N. Khandwalla, The Design of Organizations, San Francisco: Harcourt Brace Jovanovich, Inc., 1977.

the literature on corporate innovation to see how corporations have restructured themselves in the face of environmental uncertainty.

1. The Corporate Perspective

An organization's willingness to accept innovation is often referred to in organization theory as "organizational change", "organizational learning", or "organizational redesign". Over the past few years, hundreds of books have been written on how to "reengineer and restructure" corporations to take advantage of global connectivity, and make them more innovative. However, what most of these books promise is a magical recipe for creating an innovative and flexible company, rather than conducting an empirical study of processes and strategies that historically lead to innovation. The majority of what little innovation theory exists spends more time discussing barriers to innovation than it does showing keys to successful innovation.

Part of the challenge when trying to spur innovation is determining which factor or combination of factors are responsible for an organization's successful organizational innovation. Due to the complexity and size of corporations, pinpointing the reasons for successful change is difficult to do. The approach most innovation literature takes is to use case studies chronicling an individual organization's approach to innovation. Companies known for being innovative include 3M, General Motors, IBM, Motorola, and Taco Bell. These innovative companies, for whatever reasons, recognize the need to change their strategy, structure, processes, or some other aspect of their organization to adapt to a new environment. In the field of innovation theory, it is difficult to make predictions about corporate innovation. For instance, several of these innovating corporations faced decreasing performance before reengineering while some embraced innovation despite their continued success.

Much like the discussion within the national security community regarding operations in the Information Age, there is great debate in business world regarding the best way to structure a corporation to compete in today's networked society. One innovative concept, called the "virtual organization," describes an organization that focuses on its key processes (those in which it has a competitive advantage) and subcontracts other aspects of its business that can be provided better and cheaper by other companies. This approach dramatically reduces the time required to bring new products to market by creating strategic alliances that give the company flexibility in selecting its suppliers and manufacturing process. IBM's personal computer manufacturing is considered a virtual organization because it designs and manufactures computers, but it subcontracts the processing chip (Intel), operating system (Microsoft), and software (Lotus, Microsoft, WordPerfect). Being "virtual", much like the organic network described earlier, gives an organization flexibility and agility in a dynamic environment. There have been similar praises for organizations that embrace "horizontal corporations",[30] and organizations that create "lateral integration."[31]

However, others caution that the reengineering craze sweeping the business world has often met with failure, and some believe the corporate world has overreacted to the

[30] Rahul Jacob, "The Struggle to Create an Organization," Fortune, 3 April 1995, 90-99.
[31] Jay Galbraith, et al., Organizing for the Future, San Francisco, Jossey-Bass Publishers, 1993.

perceived benefits of structural reorganization. The same virtual organization that allowed IBM to design, produce, and deliver the first PC in only 15 months also launched Intel and Microsoft into corporate success that eclipses today's IBM.[32] Others argue that rather than focusing on dramatic corporate reorganization using new organizational structures, companies should focus on improving their existing hierarchical design.[33]

Despite the on-going debate, it is possible to make some broad generalizations about innovation using studies in organizational change. Many of these observations seem obvious, however it is useful to recognize what factors are involved in organizational change. When looking at large-scale organizational change, there are three factors that one must consider: the depth of change, the pervasiveness of the changes, and the size of the organization.[34] The depth of change refers to the extent to which members must shift their beliefs and values, and the degree of changes in the organization's processes. This often involves changing paradigms, core processes, organizational culture, and even missions and strategies. The greater the depth of change, the more profound the shift of the organization. However, people tend to resist change, and the deeper the change the more resistance that is likely to be encountered.[35]

Pervasiveness of change refers to the proportion of the organization that is changed. Some change only effects specific units in the organization (factories, divisions,

[32] Henry Chesbrough, and David Teece, "When is Virtual Virtuous? Organizing for Innovation," Harvard Business Review, January-February 1996, 65-73.
[33] Ashkenas, 1995.
[34] Allan M. Mohrman, Jr. et al, Large-Scale Organizational Change, San Francisco: Jossey-Bass Publishers, 1989.
[35] Ibid., 15.

geographic locations) while other change may effect specific organizational functions (hiring, information processing, rewards). The more pervasive the change—that is, the more units or functions that are affected—the greater the change to the organization. However, pervasive change is complex, long-term, and requires much coordination and cooperation.[36]

Organizational size is also a dimension in large-scale organizational change. "The larger the size of the organization, the larger the change needed to alter its character and performance."[37] There are different measures of an organization's size—including the number of employees, capacity for throughput, and assets—and each has a different influence on an organization's ability to change. Other factors, including an organization's complexity, age, culture, and level of centralization will also effect the degree of change required.[38]

So it is possible to determine, in relative terms, how dramatic and challenging change will be based on the depth of change, the pervasiveness of change, and the size of the organization. According to Mohrman et al, "as the size of the organization grows, as the change becomes more pervasive, and as the depth of change increases, the risk, difficulty, complexity, unpredictability, and intensity of the change also becomes greater."[39] But this does not explain how an organization decides to change, it only points out the challenges and factors involved once the decision to change is made.

[36] Ibid., 16.
[37] Ibid., 17.
[38] Ibid., 17-22.
[39] Ibid., 27.

Another area of study, "adaptation theory", gives some insights into the way change is initiated. It investigates the relationship between individual organizations and their environment, and supporters argue that organizations actively seek to recognize and adapt to changes in their environment. This approach suggests that successful organizations have "change agents"[40] who monitor the environment for opportunities and threats, and then formulate responses and adjust the organization's strategy, structure, or processes accordingly. Once the organization has established a new strategic vision, managers guide employees through the change at an individual level, instilling new beliefs and changing the culture of the organization. This is often referred to as "unfreezing, moving, and refreezing," as it is not enough to simply introduce change. According to Stephen Robbins, "Implicit in this three-step change process is the recognition that the mere introduction of change does not ensure either the elimination of the prechange condition or the fact that the change will prove to be enduring."[41] For adaptation theorists, change is managed and planned for rather than being accidental. In other words, organizations must consciously plans to innovate.

But there are those who study organization theory who are not as optimistic about an organization's ability to change. In contrast to the adaptation theorists who believe organizations adapt to changes in their environments, "population ecologists" believe that

[40] Change agents can include those inside the organization (senior executives, unit managers, ambitious low-level workers) or can be brought in from outside the organization (consultants, oversight committees). However, there are risks to using change agents. Internal change agents can often be biased by organizational politics, while external consultants often have little stake in the organization or are hired to validate existing policies. (Stephen Robbins, Organization Theory: Structure, Design, and Applications, 2nd ed., Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1990, 312.)

[41] Robbins, 1990, 315.

the environment selects the types of organizations that are to survive. According to the population ecologists, organizations undergo a process of natural selection as their environment changes. This Darwinian approach suggests the companies that are best suited to operate in the new environment will survive, while those that continue to operate in an outdated way eventually die off. There are several factors that preclude an organization's ability to change to meet environmental changes, including: an organization's investment in equipment and specialized personnel that are not easily transferable, internal political constraints in the organization, legal and fiscal barriers, and a general lack of information regarding environmental change.[42]

Another group of theorists takes a position between the adaptation theorists and the population ecologists. They believe that organizations remain stable over time, choosing to resist change instead of making incremental changes to match the changes in the environment. Organizations resist change because those in a position to change the organization have the most to lose by changing it, because bureaucratic organizations are designed to resist change, and because organizational cultures are so difficult to modify. But eventually the organization's performance suffers from the mismatch of structure and environment, and managers are forced to initiate revolutionary changes to adapt to the new environment.

This theory states, "Organizations are characterized by long periods of inertia, punctuated by brief periods of dramatic and comprehensive change that culminates in a

[42] Morgan, 1989, 88.

very short period of time."[43] Because change is so destabilizing and difficult to accomplish, given the choice between incremental change and radical change managers will put off action until absolute necessary. March and Simon support this theory in their book Organizations, where they state that given the choice to change or to continue operating as usual, an organization will usually choose to maintain status quo. This does not necessarily an organization will completely avoid change, it can simply mean an absence of a search for new alternatives. However, they do suggest that innovation will likely occur if the organization faces decreasing performance due to environmental changes.

One final theory, applicable to organizational innovation, bears mentioning. As previously discussed, March and Olsen's "garbage can model" refers to an organization as a solution looking for a problem. This theory predicts that innovation is unlikely because the key to problem solving is matching up the correct solution with a specific problem, not coming up with new problem-solving methods.

One common thread flows through all of these innovation theories: that innovation must be planned for and encouraged by the organization. This was the focus of a study done by Jay Galbraith who determined that innovation must be built into the core of the organization and institutionalized into its processes.[44] He makes several general statements about organizational innovation:

[43] Robbins, 1990, 327.

[44] Jay Galbraith, "The Innovating Organization," Organizational Dynamics, Winter 1982, 5-25.

1. Managers and decision makers must be aware of the difference between innovation and daily operations.

2. Separate, but connected, organizations must be established to handle each of these functions or at least differentiate between the two.

3. Organizations must have a mechanism to transfer ideas from the innovating organization into the daily workings of the operating organization..

4. Innovation must be encouraged by senior leadership who recognize the need for new ideas, and by managers who protect innovators from a system that will try to stifle change.

5. Leadership must also create an innovative culture in the organization which supports integrating new ideas into the organization.

6. The organization must recognize innovators and provide adequate rewards for those who come up with innovative ideas.

2. The Military Perspective

Having reviewed a few of the theories of corporate innovation, it is useful to point out that some of the same tendencies can be found with military innovation. In fact, it seems that the study of military innovation is, in some ways, more developed than that of corporate innovation. There have been several studies on organizational innovation in the military, but two authors stand out in their works on doctrinal innovation. Barry R. Posen, in his book The Sources of Military Doctrine[45], investigates how changes in

[45] Barry R. Posen, The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars, Ithaca, NY: Cornell University Press, 1984.

military doctrine take place. Posen investigates innovation in military doctrine between the World Wars—a period of technological change and uncertainty much like that which the United States is in now—and attempts to explain the successes of the German Blitzkrieg and the British Air Defense System, as well as the failure of the French Maginot Line. Stephen P. Rosen, in Winning the Next War, takes a much broader view of explaining military innovation. Rosen attempts to determine why military organizations make major innovations in the way they fight, and whether innovation is more likely in peacetime or wartime. He looks at twenty-one instances of innovation in the militaries of the United States and Great Britain.

Although definitions vary, military innovation can best be defined as, "a change in one of the primary combat arms of a service in the way it fights or alternatively, as the creation of a new combat arm.[46]" Both Posen and Rosen come up with several hypotheses regarding military innovation which are useful in determining whether the U.S. military, and the greater national security structure, is likely to take advantage of the opportunities presented in the Information Age and redesign itself to meet the uncertain security environment. The following are several of Posen's hypotheses about military innovation:[47]

1. Because of the process of institutionalization, which gives most members of an organization a stake in the way things are, doctrinal innovation will only rarely be sponsored by the organization itself. The hierarchical structure of the military restricts the

[46] Rosen, 1991, 7.
[47] Posen, 1984, 59.

flow of ideas from lower to higher levels, and those at the top of the hierarchy have little interest in changing the system that they have mastered.

2. Because doctrinal innovation increases operational uncertainty, and therefore makes the organization vulnerable to attack, it will rarely be sponsored by the organization itself.

3. New technology, when it has not been tried in combat, is seldom by itself a catalyst of doctrinal innovation. A new technology will likely be assimilated into an old doctrine rather than stimulate change to a new one.

4. Direct combat experience with a new technology can cause innovation. However, this does not guarantee innovation nor does it mean that the innovation will be recognized and accepted by the institution.

5. Failure on the battlefield can cause doctrinal innovation.

6. Civilian intervention can cause military innovation. This often follows a military failure causing civilians to put pressure on the military to change.

Using the cases of Germany, Britain, and France in the interwar years, Posen concludes that there was very little internally generated innovation in military doctrine. The few true innovations of the time–Germany's Blitzkrieg, the RAF Fighter Command, and the French defensive Maginot Line–were imposed from outside the defense organizations and, to some extent, resisted by the military.

Rosen, in his study, takes the question of military innovation one step further. He points out that most theories about military innovation are too general to be proven with historical evidence. First, he challenges some of the existing theories on military innovation. Although he acknowledges that military defeat has often led the organization to reevaluate its strategy, history shows defeat is neither necessary nor sufficient to produce innovation. He agrees that military organizations are unlikely to innovate on their own and usually require outside intervention for drastic change. But he also argues that civilians often don't understand how to intervene in the military, or that the military organization might regard changes as outside the purview of civilian leaders. Therefore, he suggests that innovation is generated by civilians acting together with "military mavericks"[48] in order to force innovation from within as well as without.

Rosen distinguishes between innovation in a peacetime military and innovation during wartime. Unlike most business organizations, the military bureaucracy spends most of the time not doing it's primary task of fighting foreign militaries. Because of this, Rosen believes that the military organization innovates in very different ways during peacetime than it does in wartime.

Rosen first presents some hypotheses about peacetime innovation:

1. Military innovation involves an "ideological" struggle between branches that revolves around a new theory of victory, an explanation of what the next war will look like, and how officers must fight if the next war is to be won. This requires identification

[48] A military maverick is a term used by both Posen and Rosen to denote a soldier who challenges the traditional ideas and authority of the military and uses outside forces to support their innovations. These mavericks are usually shunned by the system which they seek to change. One example of a military maverick is Admiral Hyman Rickover, credited with almost single-handedly bringing nuclear power to the U.S. Navy.

of new critical missions and new tasks to be performed, without which the innovation will remain abstract and ineffectual.

2. In the military, political power is wielded through influence over who is promoted to positions of senior command. Therefore, innovation may require the creation of new promotion pathways for forward-thinking young officers to rise to positions of power.

From this, Rosen suggests that "peacetime military innovation occurs when respected senior military officers formulate a strategy for innovation, which has both intellectual and organizational components. Civilian intervention is effective to the extent that it can support or protect these officers."[49]

Because wartime is when the military is "in business", Rosen develops separate hypotheses about wartime innovation.

1. Organizational learning and innovation will be extremely difficult if a new mission for a combat arm must be invented in order to achieve victory.

2. Innovation in wartime requires a new strategic measure of effectiveness.

3. Wartime innovation will be limited in its impact because the time required to collect, process, and distribute new information, and then create new measures of effectiveness, is too long.

[49] Rosen, 1991, 21.

4. Because innovation must be implemented in a very short period of time in order to have an impact in the war, there is an advantage to tight central command which allows for rapid reorganization once the need for innovation is perceived.

From reviewing a number of wartime case studies, Rosen finds that innovation in wartime is more difficult to predict than peacetime innovation. In some cases he found that wartime innovation was too slow to benefit military forces because of the difficulty of defining new strategic measures of effectiveness, and the absence of tight central controls to ensure implementation. He also found that innovation can occur not only as the result of analysis, but out of sheer desperation or by chance. Rosen states conclusively that "learning from wartime experience how to perform an entirely new military function was in all cases extremely difficult."[50]

Contrasting peacetime and wartime innovation, Rosen finds that innovation during peacetime has been more successful than in wartime. One difficulty with wartime innovation is the time constraint involved. Typically, organizational resistance slow the innovation process, and historically the fruits of wartime innovation come too late to be of great benefit during the conflict. Rosen concludes by saying, "In peacetime, the military has to hazard guesses about the character of future war. In wartime, the opportunity to learn from experience does exist. But the empirical record of innovation in peace and war and the hypotheses about the necessary components of wartime innovation suggest that

[50] Ibid., 180. (Although several cases in history dispute his claim.)

peacetime innovation ought to be pursued, because wartime innovation is so terribly difficult."[51]

Another noted researcher on military innovation, Williamson Murray, also studied innovation during the interwar period and sees some dramatic parallels to today. He writes, "Recent case studies of innovation in a similar period—the 1920's and 1930's—when military institutions confronted great international uncertainty, relatively low support, and substantial technological change, offer views on how one might view innovation in the next century."[52] Although he supports many of the findings by Posen and Rosen, Murray challenges some commonly accepted ideas regarding innovation. First, Murray suggests that effective military innovation is evolutionary rather than revolutionary. In his example, Blitzkrieg (already discussed as an innovation in warfare) involved a 20 year process of evaluating past failures and conducting numerous exercises. Although it appeared to be a revolutionary doctrine to the British and French during World War II, the Germans had been perfecting Blitzkrieg since the 1920's.[53] Therefore, small and gradual changes can be just as "revolutionary" as large and rapid change.

Second, Murray emphasizes that innovation, rather than being led by military mavericks, is only successful if it is embraced by the organization, thus causing a change in the organization's culture. Although Murray agrees that innovative officers can help shape the military's culture, he believes it is equally important that the organization be willing to shift its focus and accept change. According to Murray, "It thus appears that

[51] Ibid., 182.

[52] Williamson Murray, "Innovation: Past and Future," Joint Forces Quarterly, Summer 1996, 51.

[53] Ibid., 52.

long-term decisions which affect the culture and values of the officer corps are crucial to innovation, while it is difficult for a single individual to institutionalize change."[54]

Finally, Murray believes it is military culture that can either create the climate for innovation, or block innovation before it gets a chance to flourish. Murray uses the example of the Germans (who saw mistakes as a learning experience) and the British and French (who tended to downplay or suppress critical reports) to show that military culture shapes the framework used to learn from past failures. Therefore, Murray believes that exercises and wargames should be utilized to challenge existing or proposed doctrine, not to justify or "prove" it. Murray finds, regardless of the perception that armies plan to fight the last war, a desire to twist or discard history in order to justify current doctrine and beliefs. He writes, "most military organizations show little interest in studying the lessons of even recent conflicts. Rather, they ignore the past or look to another paradigm."[55]

From his studies, Murray makes several predictions and recommendations regarding creating an innovative force for today.

1. Creating detailed plans to enhance and institutionalize innovation will not be effective in promoting innovation. Rather, encouraging change in service cultures is the best route to creating an innovative force. However, this involves a long-term change which must occur at all levels.

2. Wargames and exercises should not be conducted against imaginary, ideal threats. They should reflect real opponents with real capabilities and real strategic and

[54] Ibid., 53.
[55] Ibid., 53.

political objectives. Because the value of such exercises is not in the conduct, but the lessons-learned analysis afterward, today's high operations tempo should be reduced to allow more time for debriefing and distribution of lessons-learned.

3. Similarly, lessons-learned should not be used merely to validate existing doctrine and processes. Rather than viewing failure in exercises as a failure in leadership, it should be seen as an opportunity to reevaluate doctrine.

4. In order to create an officer corps that understands history as well as operations, the services must improve Professional Military Education (PME) and make learning an integral part of an officer's career. Similarly, the services must encourage nonlinear thinking by seeking inputs from a variety of academic disciplines. Senior leaders must get past thinking of innovation in qualitative and quantitative terms and think of it conceptually.

C. CONCLUSIONS

Based on this review of organization theory, several generalizations can be made about organizational change. First, it is clear that there is a connection between an organization's environment and the organizational structure that it adopts. Whether the organization chooses to adapt to environmental changes, or a changing environment selectively enhances particular organizations, different structures have specific strengths and weaknesses depending on the environment. These strengths and weaknesses are summarized in the Table 2.2.

If the environment is static, a more bureaucratic and hierarchical organization seems to be most appropriate. However, if the environment is ambiguous and dynamic then a networked organizational structure is the best choice.

Organizational Structure	**Example**	**Strengths**	**Weaknesses**
Rigid Bureaucracy	Assembly line, small business, authoritarian government.	Efficient, reliable, precise, consistent, clear accountability.	Impersonal, detached, inflexible, obsession with control.
Senior "Management" Team Bureaucracy	Large business, department store, democratic government.	Efficient, standardized.	Inflexible, controlling.
Task Force Bureaucracy	Conglomerate corporation, federal government.	Standardized, utilizes specialized expertise.	Takes people away from assigned jobs, parochial, consensus decision making.
The Matrix Organization	Aircraft manufacturer.	Improved flexibility, interdepartmental communication, responsive.	Dual accountability, ambiguity can lead to conflict, inefficient.
The Project Organization		Dynamic, innovative, information sharing.	Ambiguous, conflictive.
The Organic Network	Fashion industry, criminal organizations.	Innovative, flexible, amorphous, shared goals, allows organization to focus on core competencies, difficult to counter.	Inefficient, ambiguous, conflictive, tendency to drift, dependency on outside organizations.

Table 2.2: Strengths and Weaknesses of Organizational Structures

Second, in order to determine which organizational structure best fits an organization, the organization must be aware of its environment and able to recognize change in a timely manner. Knowing which changes to react to and which to ignore is as important as recognizing environmental change exists. Managers must constantly compare the costs involved in reorganizing to the costs of operating with an incorrect structure.

Third, even if change is deemed necessary, an organization must be willing to innovate and restructure itself. Managers must ensure that the changes are clearly explained, coordinated, and institutionalized so that the entire organization understands and supports them. Reorganization involves changing the organization's culture and often bringing an entirely new type of worker into the organization. Finally, change is a continuing process that must be monitored and adjusted frequently. Innovation must become an integral part of the organization, and all members of the organization must constantly be looking to improve operations to fit the environment. Successful organizations must learn lessons from past failures, monitor the effectiveness of current strategies, and be on the lookout for future opportunities.

III. THE DRUG WAR

A. THREAT

> We are up against an organization stronger than the state.
> Colombian President Belisario Betancur, 1988[1]

> Drug trafficking organizations in Mexico have become so wealthy and so powerful over the years that they can rival legitimate governments for influence and control. They utilize their vast financial wealth to undermine government and commercial institutions.
> DEA Administrator Thomas A. Constantine, 1996[2]

The drug war has been waged, in some form or other, for almost a century. Rather than blaming weak laws or inadequate assistance for the failure to "win" the drug war, it is valuable to investigate the structural aspects of the drug war to determine if the United States responded to its environment using the wrong organizational structure. The purpose of this chapter is to examine the counternarcotics environment and determine if the U.S. security structure organized itself correctly to counter the drug cartels.

Webster's dictionary defines a cartel as "an industrial combination in which several different firms agree on some form of joint action.... [M]embers regain control of their own affairs instead of being directed by central management.... Cartel arrangements have commonly been made for the restriction of production and competition, joint purchase of raw materials, joint distribution of products, allocation of markets and quotas, and price

[1] Robert Filippone, "The Medellín Cartel: Why We Can't Win the Drug War," Studies in Conflict and Terrorism, Vol. 17, No. 4, October 1994, 324.

[2] DEA Congressional Testimony, Drug Trafficking in Mexico, 28 March 1996, 5.

fixing." This basically fits the description of the transnational drug trafficking groups today.

Man has been dealing with the negative effects of illegal drugs for centuries. But the drug cartels, coalitions of drug dealers who pool resources and split profits, have been a relatively new development that has increased both the wealth of drug dealers and their threat to U.S. national security. The drug cartels, much like successful corporations, have adapted to the Information Age by flattening their organizational structure and increasing flexibility. In the past 20 years, transnational drug trafficking groups have turned from highly bureaucratic and independent organizations into highly networked and interdependent ones. Because of the violent means the cartels use, and the threat drugs pose to U.S. citizens, drug cartels top the list of Information Age threats to U.S., and global, security. Referring to the drug cartels, DEA Administrator Thomas Constantine says "[t]hese individuals, from their headquarters locations, absolutely influence the choices that too many Americans make about where to live, when to venture out of their homes, or where they send their children to school."[3]

In the days before the cooperative arrangement of the drug cartels, drug lords were organized as independent entities operating with their own resources and often competing against each other for markets and resources. Individually, the drug organizations were organized hierarchically with a family head and multiple layers of management. However, with the birth of the Medellín drug cartel in 1981, the narcotics

[3] DEA Congressional Testimony, Mexico and the Southwest Border Initiative, 25 February 1997, 2.

organizations began to take on a new organizational structure. By pooling resources, sharing smuggling routes, and ruling by consensus, the drug cartels took on the networked structure that still exist today.

Due to the extreme secrecy surrounding drug cartels' operations, it is difficult to accurately map out their organizational structure. However, from open-source literature based on informants, failed smuggling activities, and congressional testimony, it is possible to piece together a picture of what the cartels' structure looks like. The drug cartel network extends to all levels of society and almost every geographic region of the world; however, this paper will focus mainly on the Latin American drug trade. Although there are a variety of illegal narcotics entering the United States from Latin America, this study will mainly address the cocaine trade, the drug cartel's "product-of-the-day".

1. The Global Drug Network

It is important to realize that the drug problem is a global one. No part of the world is untouched by illegal drugs, and virtually every country is involved in either the production, transport, or distribution of illegal drugs. It is in fact a mistake to highlight individual countries as being the "root" of the problem with drugs, for drug organizations operate in a "borderless" world

At one time in history, the drug problem could be considered a marginal area of criminal activity. But the lucrative nature of the drug trade has forced a change of the narcotics business into a major global enterprise.[4] Total sales of illicit drugs worldwide is estimated at $180 billion-$300 billion annually.[5]

Historically, regional drug trafficking groups focused on one particular part of the illegal drug market. Heroin and morphine, derived from the opium poppy, originated mainly from the "Golden Triangle"[6] countries of Southeast Asia and the "Golden Crescent"[7] countries of Southwest Asia. Cocaine production, derived from the coca plant, originated almost entirely in the Andean countries in South America.[8] Marijuana and hashish, from the cannabis plant, was largely global in nature although certain regions were renowned for their particularly potent crops.[9]

Since the late 1980s, however, there has been a trend toward globalization of the drug trade. Several established drug organizations have recently diversified into other markets. For example, Colombian cartels have recently begun growing and processing opium, and are attempting to seize the U.S. heroin market with a cheaper and significantly more pure product.[10] At the same time Lebanon, in the Middle East, and Bolivia and Peru, in Latin America, have developed the capability to process cocaine base into cocaine powder, a process traditionally done in Colombia.[11]

[4] Paul B. Stares, Global Habit: The Drug Problem in a Borderless World, Washington, DC: The Brookings Institution, 1996, 1.
[5] Ibid., 2.
[6] The Golden Triangle consists of Laos, Thailand, and Burma.
[7] The Golden Crescent is made up of Afghanistan, Pakistan, and Iran.
[8] Includes Peru, Bolivia, and Colombia.
[9] Stares, 1996, 2.
[10] According to the DEA (DEA Congressional Testimony, The Threat of Heroin to the United States, 19 September 1996,) in order to seize the U.S. heroin market, the Colombians' provided heroin that was 80-99 percent pure (up from approximately 5 percent purity a decade ago) at approximately 50 percent of the cost. This high-quality heroin can be smoked or snorted instead of injected.
[11] Stares, 1996, 3.

International trafficking and marketing of drugs is another area that has become even more global. As international trafficking routes shift to new countries, unexplored markets open up for selling illegal drugs (and because they are not subject to tax or tariff, opportunities in illegal trade are even greater than for legitimate trade.) As borders become more open, and free trade zones encourage greater international trade, drug trafficking will likely become even more widespread and difficult to detect.[12]

The globalization of the drug trade makes fighting the drug cartels even more challenging. Drug cartels have typically operated from countries where they can avoid prosecution by law enforcement officials. Even assuming foreign governments are able to organize effective counter-narcotics efforts, it is likely that drug cartels will shift operations to other, less stable countries. Paul Stares writes, "Given the threat of legal sanctions, suppliers are risk typically risk averse, seeking places to operate where law enforcement is less effective or nonexistent… Although government authority may be strengthened in some areas, the opposite is also likely to be true in others as a result of civil war and domestic unrest, which provide ample opportunities to produce illicit drugs."[13] Thus, the global nature of the drug problem likely requires a global response. Otherwise, criminal organizations will simply operate out of nations that will not, or cannot, enforce laws.

Due to the enormity of the problem, this study will focus on narcotics trade in the western hemisphere. Despite the limited scope of this case study, the Latin American drug

[12] Ibid., 7.
[13] Ibid., 48 and 86.

cartels and the North and South American response are very typical of the battle between drug organizations and security organizations worldwide. Also, of all the drug organizations worldwide, the proximity of the Latin American drug cartels pose the greatest threat to U.S. national security.

2. History of Narcotics Trade in the Western Hemisphere

The Latin American drug cartels, in the form we know them today, have only existed since the 1980s. However, the problems associated with drugs in the Western Hemisphere have existed for centuries. The ancient tribes of Latin America, such as the Inca, used the coca leaf for religious purposes and as a stimulant. In those times, coca was cultivated just like other staple crops, such as manioc and sweet potato.[14] Despite the historic ties Indians had to the coca leaf, the early Spaniards tried to combat the use of coca. Latin American governments later tried to fight cocaine, developed in 1920, without success. In 1947, Colombian President Mariano Ospina outlawed the cultivation and consumption of both cocaine and marijuana, but like the United States' alcohol prohibition laws he was soon forced to repeal the law due to public outcry.[15]

Problems in the United States with illegal drugs from Latin America began to emerge in the 1960s. Cuba, during the 1950s, was a well-known center of corruption and violence. The Cuban Mafia imported small amounts of cocaine for sale as a "luxury drug", using Colombians as couriers. However, when Fidel Castro came to power, many of the Mafia members resettled to Florida. They maintained their ties to South American

[14] Scott B. MacDonald, Mountain High, White Avalanche, New York: Praeger, 1989, 5.
[15] Ibid., 6.

cocaine producers, and eventually realized the potential for much wider marketing in the United States.

In the 1960s, Colombia was the major production and trafficking point for marijuana. Eradication efforts in the early 1970s virtually destroyed Colombia's marijuana production, but narcotraffickers learned a valuable lesson from their Cuban ties. They shifted their production to cocaine, which was easier to transport and much more profitable than marijuana, and moved their production deep into the jungles and away from government control. Fueled by increasing demand in the United States, the cocaine trade grew rapidly, netting huge profits for the drug traffickers. Like any business leaders, the narcotraffickers reinvested large sums into building up a production and transit infrastructure, but unlike legitimate businesses they used extreme violence to neutralize the competition. Because of their previous experience trafficking marijuana, the Colombian narcotraffickers already had established supply routes and distribution contacts to work with. By the late 1970s, the Colombians began to set up their own networks in the United States, bypassing the Cuban connection they had previously worked through. This led to a bloody turf war in south Florida that saw the Colombian narcotraffickers emerge in control of the cocaine industry.

The Cali and Medellín cartels rose in strength throughout the 1980s and early 1990s. It is estimated that by 1990, Colombian illegal drug profits amounted to over $6 billion a year. In 1988, three of the cartel heads made the Forbes magazine list of the 125 non-U.S. billionaires. However, in the early 1990s the United States and Colombian government made considerable inroads in arresting or killing the most visible leaders of the Colombian cartels.

Until recently, Mexico only played a secondary role in the trafficking of drugs to the United States. Because of its proximity to the United States, Mexico has always been a significant point of entry for all kinds of illegal drugs. There has been tension between the United States and Mexico over drug smuggling efforts ever since the 1930s when the Mexican government banned cultivation or export of marijuana. In the late 1970s, the United States and Mexican governments coordinated their eradication efforts, and the supply of Mexican marijuana in America fell from more than 75 percent in 1976 to around 11 percent in 1979.[16]

This gap in marijuana production and export was replaced by transit of cocaine from Colombia. During the 1980s, Colombian cartels transported drugs by air and sea mostly using established routes through the Caribbean. In the mid-1980s the United States launched efforts to interdict the flow of drugs coming through the Caribbean, and the cartels shifted their transit routes into Mexico. Because of Mexican traffickers' previous experience smuggling marijuana, the arrangement favored both the Colombian cartels and the Mexican smugglers. The DEA estimates approximately 70 percent of cocaine entering America transited through Mexico in 1996.[17]

[16] Miguel Ruiz-Cabañas, "Mexico's Changing Illicit Drug Supply Role," in The Drug Connection in U.S.-Mexican Relations, ed. Guadalupe Gonzáles and Marta Tienda, San Diego: Center for U.S.-Mexican Studies, 1989, 48.

[17] U.S. Government Accounting Office, Drug Control: Counternarcotics Efforts in Mexico, GAO/NSIAD-96-163, June 1996, 3.

Historically, Mexican transports were paid in cash, netting about $1000-$2000 dollars for each load they smuggled into the United States.[18] By the early 1990s Colombian cartels and Mexican traffickers came to a new arrangement. Instead of turning all the smuggled cocaine over to the Colombian distribution network, the Mexicans would receive half of every drug shipment they smuggled to distribute on their own. This led to an increase in profit for the Mexican traffickers by approximately 1000 percent, and it gave birth to a new breed of Mexican drug cartels, sometimes called "the Federation."[19] The Mexican cartels and the Colombian cartels have parallel, but separate, distribution networks for cocaine in the United States. According to the Drug Enforcement Administration, Mexico has once again become the largest foreign supplier of marijuana and is a source country for heroin. According to the Administrator of the DEA, "I am not exaggerating when I say that these sophisticated drug syndicate groups from Mexico have eclipsed organized crime groups from Colombia as the premier law enforcement threat facing the United States today."[20]

Despite their already enormous influence and profit, the drug cartels are attempting to expand their influence and diversify their operations. Latin American cartels have expanded their smuggling routes through Eastern Europe and Africa,[21] and they have

[18] Drug Control in the Western Hemisphere, 1996, 4.

[19] "The Federation" is made up of four major cartels: The Tijuana Organization, The Sonora Cartel, The Juarez Cartel, and The Gulf Group. It is debated how much these organizations coordinate their activities or compete with each other.

[20] Mexico and the Southwest Border Initiative, 1997, 1.

[21] According to an essay in the Christian Science Monitor (Robert Rothberg, "They Slip Out of Nigeria and Drug the World," 24 September 1996, 19), "limited detection and ease of access to Europe has made southern Africa a drug crossroads, with heroin flowing west and cocaine east." The emergence of Africa as a drug transit point has prompted the DEA to open up a regional office in Johannesburg, South Africa.

made strategic alliances throughout the world. Colombian and Mexican cartels are also shifting production to other drugs. In 1989, 94 percent of the heroin seized by U.S. law enforcement came from Asia. By 1995 over 60 percent of the heroin seized came from Latin America.[22] Pound for pound, heroin is ten times more profitable than cocaine and just as easy to transport. Additionally, in the past three years the Mexican cartels have shifted their efforts toward the production of methamphetamine, a market previously controlled by Hell's Angels in the United States. Although the Mexican cartels are just one link in the cocaine business, they now control the entire methamphetamine production and distribution process.

3. Cartel Structure

Prior to 1980, the Colombian narcotraffickers operated largely independent of each other, and in fact often engaged in turf battles using their well-armed private armies. In 1976 a small-time drug smuggler named Carlos Lehder Rivas brought a new idea to one of the most powerful narcotraffickers in Colombia, Jorge Luis Ochoa. Instead of using "mules" (smugglers carrying small amounts of drugs on their person) to transport cocaine, Lehder envisioned using small, private aircraft and boats to smuggle larger amounts of the drugs covertly.[23] With this revolutionary idea, the Ochoa-Lehder organization quickly became the top exporter of cocaine to the United States. In 1977, the DEA opened file on the "Medellín Trafficking Syndicate."

[22] The Threat of Heroin to the United States, 1996, 3.
[23] MacDonald, 1989, 21.

The first "drug cartel" was formed in 1981 in the town of Medellín, although the Colombian narcotraffickers had loose ties to each other prior to that point. The Medellín cartel did not unify in order to consolidate power or combine production efforts. The Medellín cartel first formed in response to the kidnapping of Marta Ochoa, Jorge Luis' sister, by the insurgent group M-19. Throughout Latin America, kidnapping wealthy people and demanding huge ransom was used by guerrilla groups to raise funds for their cause. At the request of the Ochoa family, over 200 of Colombia's most influential narcotraffickers met in Medellín on 12 November 1981. The group recognized the danger they faced from these guerrilla groups, and understood the consequences that would result if they set a precedent by paying ransom to M-19.[24]

In response, the narcotraffickers each donated $7.5 million to form a right-wing paramilitary group, called *Muerte a Secuestradores* (MAS, or "Death to Kidnappers"), to fight the insurgents.[25] This pivotal event brought a loosely-connected group of narcotraffickers together into a coordinated and powerful force, known as the Medellín cartel. Although originally intended to be a unified defense of their organizations, cartel cooperation quickly extended to every aspect of the trade; from something as complex as building underground production facilities to something as simple as making sure no aircraft or ship transported less than a full load of drugs in order to maximize profit and minimize risk. This agreement to coordinate activities and share resources marked a definite shift from a hierarchical organizational structure to a more networked structure.

[24] Filippone, 1994, 325.

[25] Ibid., 325.

Although the Medellín cartel was the largest of the Colombia cartels, the smaller Cali cartel operated in a similar manner and gained strength following the arrest or death of several Medellín cartel leaders. Over the past five years the, Colombian government has made significant advances in breaking up the Medellín and Cali cartels. In 1995, six of the seven top leaders of the Cali cartel either surrendered or were arrested,[26] and the last of the Cali cartel leaders surrendered to police on 2 September 1996. With the Cali cartel supposedly gone, many hoped Colombia's drug trafficking problem would significantly decrease. However, the vacuum left behind by the Colombian cartels was quickly filled by new, younger drug traffickers in both Colombia and Mexico. According to the DEA, "In the transition stage since the Cali arrests, we have seen the same patterns of violence we observed in the La Cosa Nostra when the families fought to claim territory from fallen family leaders."[27] Additionally, leaders of the Cali cartel quickly established relationships that allowed them to regain control over large portions of their organization from prison.

Over the past decade, the Colombian and Mexican cartels have spread their tentacles throughout the entire world, expanding into areas far outside the drug trade including politics, contraband, and even slavery.[28] But it was illegal drugs that made the

[26] Anita Snow, "U.S. Lauds Colombia, Mexico for Drug-War Efforts," The Fresno Bee, 24 April 1996.

[27] Drug Control in the Western Hemisphere, 1996, 3.

[28] According to a Time magazine article entitled "Animal Genocide, Mob Style," (Michael Lemonick, 14 September 1994, 77) South American drug cartels often smuggle exotic birds and snakes on the same planes that they transport drugs. The cartels started in the illegal wildlife trade first by using the animals as live vessels to carry drugs, killing the animals to get the drugs when they reached their destination. However, the cartels realized the huge profits involved with exotic animal smuggling and have "diversified" their operations.

cartels what they are today, a $6 billion dollar international enterprise that re-invests over half its profits into Latin America's economy[29].

The Colombian government has collected enough intelligence about the drug cartels to estimate their organizational structure as shown in Figure 3.1.[30]

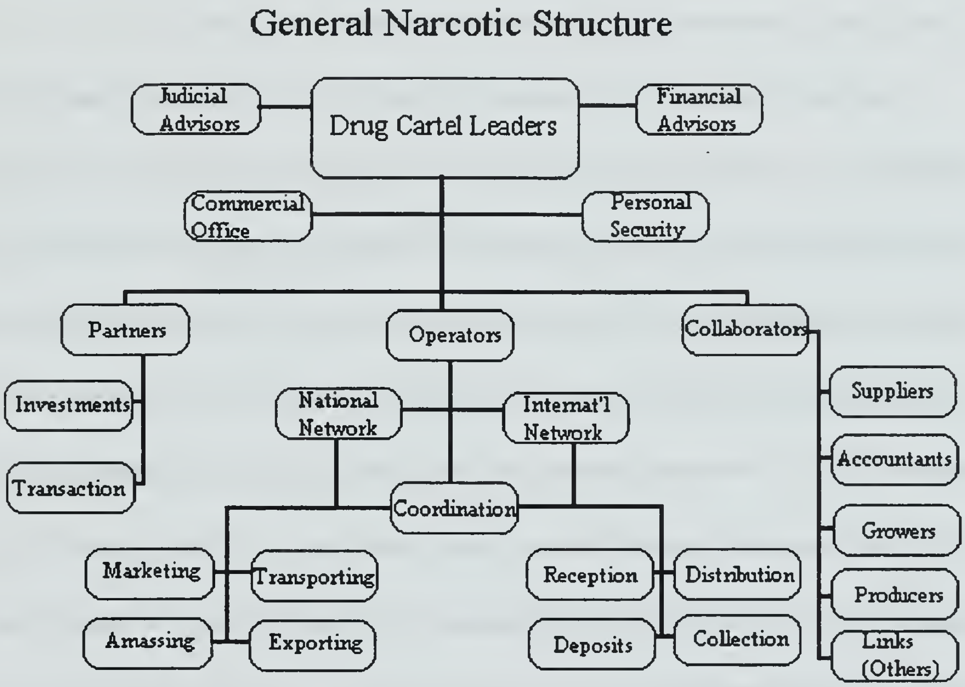
General Narcotic Structure

Figure 3.1. Drug Cartel Organization (Hierarchical)
"Inside Colombia: Bridge to South America"

Yet this diagram is misleading in that it shows the drug cartels to be hierarchically structured, with numerous levels of command and coordination. Perhaps this is the way it

[29] Francisco Thoumi, "The Economic Impact of Narcotics in Colombia," in Drug Policy in the Americas, Peter Smith, ed, Bounder, CO: Westview Press, 1992, 70.
[30] Taken from an English translation of "Inside Colombia: Bridge to South America," a document written by the Colombian government to document its efforts fighting narcotics. The entire report can be found in an Air Command and Staff College paper entitled "Information Warfare and Counterdrug Operations".

was in the early 1980s, but over time the cartel structure seems to have taken on a networked form of organization, with decreased decision making authority at the top and free-flowing communications between all members. Increases in information technology and the wealth of resources available to the drug cartels have allowed them to shift their structure away from the hierarchical model described in Figure 3.1.

Unlike a hierarchical organization, cartel leaders come and go with very little overall impact on the organization. Drugs are continually processed and transported in a highly efficient manner, yet the organization is flexible enough to shift production sites or trafficking routes as law enforcement efforts target specific parts of their operation. Although the drug cartels originally learned how to operate from the hierarchically organized Mafia, the cartels "seem to be more amorphous than criminal organizations in the United States or Western Europe. Their boundaries are fluid, the cast of characters change continually, and the links in the chain are bound together by an intricate system of contracts and subcontracts."[31]

In order to see the true structure of the drug cartels, it is helpful to map out the process that is involved with producing, transporting, and selling cocaine. The cocaine network starts with farmers in Peru, Bolivia, Ecuador, and Colombia growing coca plant for their leaves. Coca grows well in any climate, especially in mountainous regions where other crops cannot survive, making coca the most profitable crop in the region.[32] The

[31] Rensselar W. Lee, III, The White Labyrinth: Cocaine and Political Power, New Brunswick, NJ: Transaction Publishers, 1990, 99.

[32] For comparison sake, a hectare of coca leaf in 1992 would net a profit of $4,340 for a farmer in the Chapare region of Bolivia. The same hectare of land would net a $800 profit for coffee, $2,000 for citrus

harvested coca leaves are then picked up at the farms by smugglers and sent to one of many local processing laboratories where the coca leaves are mashed and soaked in kerosene and sodium carbonate. This results in a semi-processed coca paste that is packaged and transported to larger, regional processing labs. There, the coca is mixed with sulfuric acid and potassium permanganate to make an impure cocaine base. The cocaine base is then transported via a network of air, water, or land routes to high-technology labs hidden in the Colombian jungles. There, it is mixed with more expensive chemicals like acetone and hydrochloric acid (also smuggled into Colombia illegally) and dried into powder form, called cocaine. At the laboratories the cocaine is packaged and smuggled north, again by a vast network of land, water, and air routes, through Central America, Mexico, and the Caribbean. Cocaine is then smuggled, using a variety of means, into the United States, where it is distributed to cutters who dilute the cocaine with additives and package it for individual sale. The individual packages of cocaine are distributed to drug dealers for sale, or further processed into "crack" cocaine.[33]

In addition to employing those who deal directly in cocaine processing, the cartels also employ a huge number of support personnel creating jobs for contract killers, security forces, lawyers, construction personnel, cooks, accountants, etc. The cartels control everything that goes into supporting and maintaining drug production and marketing, yet they subcontract for most of it. Many of the jobs created require highly specialized skills, and it would be cost ineffective (and unnecessary) to employ them full-time. As one

fruits, or $2,700 for cacoa. (Flavio Machicado, "Coca Production in Bolivia," in Drug Policy in the Americas, edited by Peter Smith, San Francisco: Westview Press, 1992, 92.)

[33] U.S. Department of Justice, Drugs, Crime, and the Justice System, December 1992, 42.

RAND researcher points out, "[t]he cocaine trade employs, directly and indirectly, over 200,000 people in Colombia, making the industry one of the single largest employers in the country."[34] If one includes farmers, laborers, processors, and smugglers in Peru, Bolivia, and Colombia the figure rises to an estimated 1 million people employed by the drug cartels.[35]

Communications and decision making take place at all levels, and between practically every aspect of the drug trade. Instead of being strictly hierarchical, where for example, the smugglers have no contact with the farmers or the distributors, the drug cartels' structure is closer to an organic network where constant communication is necessary between all parts of the organization that overlap. Additionally, like the fashion industry example in Chapter III, the drug cartels do not so much produce a product as they integrate the various aspects of the illegal drug trade. Therefore, it is helpful to add the additional relationships to the organizational diagram to show the true nature of the drug cartel's organization, as seen in Figure 3.2.

[34] Kevin Jack Riley, The Implications of Colombian Drug Industry and Death Squad Political Violence for U.S. Counternarcotics Policy, N-3605-USDP, RAND report, Santa Monica, CA: RAND, 1993, 15.
[35] Drugs, Crime, and the Justice System, 1992, 36.

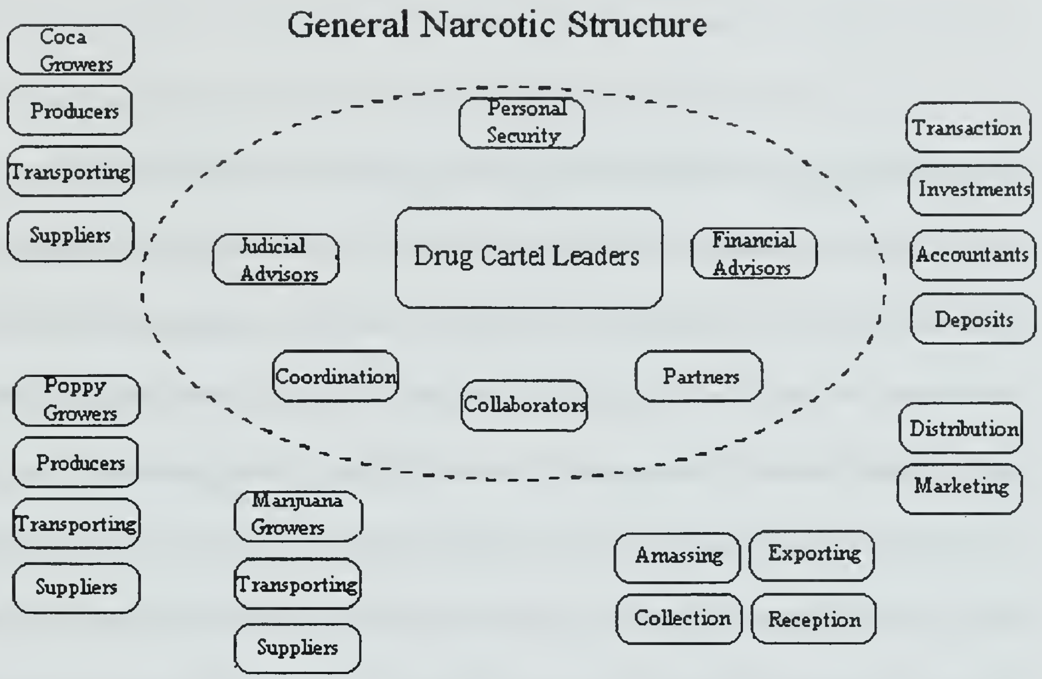

Figure 3.2. Drug Cartel Organization (Networked)

From this diagram it is easy to see why the drug cartels are not hierarchically organized. The drug cartels fit Morgan's description of an "organic network", with a core staff who sets the strategic direction for the organization (cartel bosses decide what to produce and where to market it) and numerous individuals and organizations who are subcontracted to manufacture, protect, transport, and market the product. The cartel network is held together by a product (currently marijuana, cocaine, and heroin) and the loose structure encourages flexibility and innovation at all levels. As evidenced by the continuation of the cartels even after every leader of the Medellín and Cali cartels were jailed or killed, the cartel network does not have a "head" that can be removed but contains a vast network of parts that can be removed and replaced as needed.

a. *Command and Control*

As with other networked organizations, decision making authority in the drug cartels is pushed to the lowest levels of the operation. While the leadership of the cartels is typically made up of family heads, entry into the drug organization is based on ability and interest, not on family membership. At the "core" of the drug cartel are the family heads and cartel bosses who give strategic guidance to the organization. Due to the highly complex nature of drug production and trafficking, it is highly unlikely that the cartel leaders get involved in the minutiae of the operation. Instead, operational decision making is passed down to junior members of the operation. Members maintain contact with each other using a variety of high-tech devices including fax machines, cellular phones, e-mail, and pagers. Their communications are coded and changed frequently, making it difficult or impossible for law enforcement officials to gather information.

The production, processing, and transport of cocaine involves highly complex and interdependent relationships between the farmers, transports, processors, smugglers, and distributors. Each must be in constant communication with the other to ensure a efficient flow of drugs to suppliers. Often times shipments of drugs are split into numerous, smaller shipments for transport and then reassembled in the United States for shipment and sale. The networked structure of the drug cartels allows each part the flexibility to adapt to the situation, and remain in contact will all other parts involved in the process. Because of the need for security, members often do not know the identities of other parts of the organization. Yet the anonymity of cellular communications, and the widespread availability of e-mail, makes anonymous communications a simple matter these days.

One way the United States has sought to destroy the drug cartels is by targeting their command structure. When fighting hierarchical organizations, "counterleadership targeting" is often successful in breaking the chain-of-command to the point where command and control of forces is impossible. Many thought the December 1993 death of Medellín cartel boss Pablo Escobar would mean the end of Colombian drug trafficking. However, in the past three years the United States and Colombian governments have either arrested or killed virtually every leader of the Medellín and Cali cartels with little overall impact on the organizations. Like the Hydra of Greek mythology, when the heads of the two most powerful drug cartels in the world were cut off, many more sprung up to fill the gap.

Today the Colombian cartels still exist[36], though they are not nearly as powerful as they once were. But dozens of "baby cartels" have recently emerged. Many of these cartels are led by lower-level officials of the Colombian cartels while others, such as the Mexican cartels, have emerged from other parts of the operation. Not only are these new groups harder to find (for decades intelligence efforts were focused only at the top-level command) but they are even smaller and more flexible than past cartels.

[36] According to a 10 December 1996 Santa Fe de Bogota Inravision Television broadcast, Colombian National Police discovered several Cali cartel bosses held in a top security section of La Picota Jail in Bogota had set up a network of contacts operating that allowed them to continue operations.

According to a 1995 Newsweek article, "agile and savage baby cartels have sprung up, eager to move into the breach opened up by the capture of the Cali capos."[37]

Despite these lessons, the U.S. continues to target the cartels' command and control structure. For the past three years, the Southwest Border Initiative[38] has attempted to map out the Mexican cartels' structure using communications intercepts, and then target the senior U.S.-based leadership for arrest and incarceration. But the transnational nature of the drug cartels has made it possible for virtually all identified cartel leaders to operate with impunity out of Mexico or other Latin American countries.[39]

b. *Intelligence*

The drug cartels have two methods of gathering and passing intelligence. First, they employ the highest technology equipment to eavesdrop and gather intelligence on government counternarcotics operations. Drug cartels are able to use their vast wealth to invest in the latest technologies including computers, telecommunications equipment, GPS receivers, and much more. Although most information regarding cartel collection capabilities is classified, the availability of high-quality commercial satellite imagery and unclassified news services makes it likely that the cartels are just as capable as the intelligence organizations they are competing against. It is known that the cartels' intelligence arms function much like the intelligence services of many countries. According to Senator John Kerry, former Chairman of the Senate Subcommittee on

[37] David Schrieberg, "Birth of the Baby Cartels," Newsweek, 21 August 1995.
[38] A program that coordinates the efforts of the DEA, FBI, the United States Attorney's Office, the Criminal Division, the U.S. Border Patrol, the U. S. Customs Service and state and local authorities in the fight against drug trafficking across the U.S.-Mexico border.
[39] Mexico and the Southwest Border Initiative, 1997, 2.

Terrorism, Narcotics, and International Operations, "they compartmented their activities, paid for information, and placed spies in their opponents' forces, especially law enforcement. Like intelligence agencies, they got access to telephones, tapped trunk lines out of Colombia, and used special software to analyze who was calling the American Embassy and the Drug Enforcement Administration."[40]

The second way the cartels gather intelligence is through the use of threats and money to corrupt military, law enforcement, and government personnel. The Colombian drug cartels learned the art of intimidation from the Italian Mafia operating in the United States. They adopted, and refined, the practice of offering "plomo o plata", literally lead or silver. Death or money.[41] Politicians, police officials, and military personnel are paid relatively large sums of money to protect the cartel's organization as well as to provide advance warning of counternarcotics efforts. Those who stand up to the cartels are usually killed in the most gruesome and public means possible.

The cartel's intelligence network includes, "informants strategically placed in police organizations, the military, and key government ministries such as Justice, Interior, or Foreign Relations.... Cocaine syndicates reputedly have informants inside U.S. embassies in drug producing countries (and) U.S. narcotics experts in Bogotá have speculated that the cocaine mafia might have access to some of the U.S. embassy's cable traffic."[42]

[40] Sen. John Kerry, The New War: The Web of Crime That Threatens America's Security, New York: Simon and Schuster, 1997, 74.
[41] Lee, 1990, 10.
[42] Ibid., 106.

Aside from using violence, the relatively low pay of Mexican police makes it easy for the cartels to buy information and protection at the all levels. In November of 1995, a large cargo plane, reportedly transporting up to 17 tons of Colombian cocaine, landed in Baja California and was off-loaded with the assistance of local Mexican Federal and State Police.[43] The U.S. government has generally lauded Mexico for its dedicated anti-corruption campaign, but many Mexican officials point out corruption has been part of the Mexican society for generations.[44] Many believe it is up to the military, seen as the least corrupted institution in Mexico, to stop corruption and fight drugs. In December 1995, a contingent of Mexican military were sent to Chihuahua to replace 60 judicial police accused of corruption.[45] However, the arrest of the top anti-narcotics official, General Jesus Gutierrez Rebollo, for ties with drug cartels in February 1997 showed that virtually no one is immune from the corruption of the drug trade.[46]

c. *Alliances*

Drug cartels, though intimidation, corruption, and payoffs, have made alliances with virtually every aspect of Latin American government and society. Cartels lobby governments, employ informants, buy security, and bribe officials in order to protect their business interests.

Recent events in Colombia and Mexico, including charges that President Samper accepted up to $6 million during his 1994 election campaign and the arrests of

[43] DEA Congressional Testimony, Drug Trafficking in Mexico, 28 March 1996, 5.

[44] Drug Control: Counternarcotics Efforts in Mexico, 1996, 9.

[45] Ibid., 8.

[46] "Mexico Drug Czar Ousted," Associated Press, 18 February 1997.

several high-level Mexican counternarcotics officials, show just how powerful the cartels have become. Although the Mexican Federation is a relatively new phenomenon, Mexican drug traffickers have also used money and threats to corrupt government officials and police for years. One recent example occurred in Mexico City in 1994, when two groups of police engaged in a gun battle over the arrest of a drug trafficker. One group wanted him arrested, and the other presumably wanted him released.[47] As in Colombia, numerous justice officials and anti-drug politicians have been assassinated for challenging the cartels. The murders of two high-level PRI officials, Secretary-General Francisco Ruiz Massieu, and presidential candidate Luis Donaldo Colosio, remain unsolved. Both were anti-drug crusaders who vowed to fight corruption in the government. During 1996, seven top law enforcement officials in the Baja region were assassinated. This indicates the lengths the Mexican cartels are prepared to go to protect their business interests.

Despite the fact that the Colombian cartels originally formed to counter the threat from guerrilla groups, the drug cartels have been equally willing to employ leftist groups for protection of crops, drug labs, and air strips. There is strong circumstantial evidence that the M-19's storming of the Colombian Supreme Court was ordered by drug cartels in order to destroy evidence and intimidate judges. In September 1996 two Colombian guerrilla groups, the *Fuerzas Armadas Revolucionarias de Colombia* (FARC, or Revolutionary Armed Forces of Colombia) and *Ejército de Liberación Nacional* (ELN, or National Liberation Army), supported local farmers protesting the government's crop

[47] Harry Sterling, "Mexican Bloodshed Reveals New Crisis, Drug Anarchy Could Follow Weakening of PRI's Iron Control," The Toronto Star, 7 October 1994.

eradication efforts.[48] Either in support of the farmer's protest, or in retaliation for the deaths of several protesting farmers, the insurgent group FARC launched the most deadly anti-government attack in its 40 year war against the government.[49] According to the Colombian government, the FARC has gone from supporting existing drug cartels to producing and transporting drugs on their own, perhaps even becoming the main cartel in Colombia today.[50] In its negotiations with the Colombian government over the release of 60 kidnapped soldiers, the FARC was successful in getting military forces to withdraw from Remolinos del Caguán, "one of the principle cocaine cultivation, processing, and trafficking regions" in Colombia.[51] This merging of guerrilla and criminal drug activity makes combating the group even more difficult, as the methods used to deal with insurgent activity are very different than those used to deal with criminal activity.

The drug cartels, through widespread corruption, have also gained support of the Colombian and Mexican governments. In 1979, the United States and Colombia drafted an extradition treaty allowing drug traffickers to be extradited to the United States for trial and punishment. Extradition is the greatest fear of the drug cartels. Cartel leaders know their influence and money will provide them protection from conviction or punishment in Latin America. But their political control does not extend to the United

[48] "Guerrilla Offensive Inflicts Big Losses," Latin American Weekly Report, 12 September 1996.
[49] Pamela Mercer, "Rebels Kill 80 in Strongest Attacks in Colombia in Decades," New York Times, 2 September 1996.
[50] Statement of General Harold Bedoya Pizarro, General Commander of Colombian Military Forces, before the House Subcommittee on National Security, International Affairs, and Criminal Justice, 14 February 1997.
[51] Ibid.

States, and so extradition would effectively put them out of business.[52] Leaders of the Colombian cartels, calling themselves "The Extraditables," immediately organized an effort to fight the extradition treaty. Colombia's drug cartels were so concerned about extradition that they attempted to negotiate directly with the Colombian government.

Following a government crackdown on the cartels in 1984, cartel leaders contacted former President Alfonso López Michelsen in Panama, claiming to represent 80 percent of Colombia's narcotraffickers. In exchange for exemption from the 1979 Extradition Treaty, the cartels would give the government $3 billion annually to support the economy. Additionally, they would dismantle the cartels, assist in rehabilitation of addicts, and aid in crop substitution to replace coca with other products.[53] The Colombian government turned down the offer, but it shows how far the cartels were willing to go to maintain power. The 1979 Extradition Treaty was eventually signed, but Colombia did not extradite any drug traffickers until January 1985. This sparked a war between the cartels and the government that eventually led Congress to declare the treaty "unconstitutional" in 1991. It is now illegal for the Colombian government to extradite convicted drug traffickers to the United States for incarceration, a law the United States wants changed as an act of good faith.

[52] Although recent reports show that the corrupting effect of drugs has spilled over into the United States. According to a 1 March 1997 article from the Associated Press, in 1996, the Justice Department's Office of Inspector General launched 110 new investigations into border corruption in the Immigration and Naturalization Service. In the last three years, 28 state and federal officials have been indicted on border-related corruption charges.

[53] MacDonald, 1989, 39.

Similarly, intimidation and corruption has resulted in the legal system being overly accommodating to drug traffickers. As an incentive to get drug traffickers to surrender voluntarily, the Colombian government offered to halve the jail-term for anyone who confessed, and allowed time off for good behavior. This led to cartel bosses serving only 5 years before being released to pick up right where they left off, with all their drug profits intact.[54] Even in prison, cartel leaders continue to run drug trafficking operations unhampered. According to Colombian police, "Cali Cartel bosses who are interned in the top security section of La Picota jail handle an internal infrastructure that has permitted them to continue committing crimes from inside the penal facility.... These liaisons, together with the help of other inmates, had allowed the Cali Cartel operations to resume."[55]

Additionally, the Colombian cartels have attempted to gain the support of the masses. Pablo Escobar was widely known for financing widespread renovations of the slums surrounding Medellín. His project, "Medellín Without Slums", constructed over 450 housing units for poor families, built soccer fields, and replaced water and sewage lines in many areas ignored by the government.[56] The cartels have tried to convince the populace that drugs are a product with a huge international market that can bring in much needed money and reduce unemployment.

[54] Juanita Darling, "Short Prison Terms of Freed Drug Lords Rile Colombians", Los Angeles Times, 21 September 1996.

[55] "Police Discover Cali Cartel Operations Inside Picota Jail", Santa Fe de Bogota Inravision Television Canal, Foreign Broadcast Information Service, 10 December 1996.

[56] Filippone, 1994, 5.

The cartels have sought to enmesh themselves into the entire fabric of Colombian society. While the vast majority of the Colombian people detest what is happening to their country, cartel leaders have entered in to legitimate markets in an attempt to expand their power. For example, Colombian cartel boss Carlos Lehder bought into major local radio stations and newspapers. He even created his own political party, the Latin Nationalist Movement (MLN), to spread his nationalist ideology.[57] In 1982 Medellín cartel leader Pablo Escobar was elected as an alternate to the Colombian House of Representatives, partly because if his "social programs" that included handing out money at campaign rallies and launching "Medellín without Slums". In 1983 the Colombian government announced the drug cartels had spread their influence to sports, with direct ties to 6 of the 14 professional soccer clubs in the country.[58]

The cartels have become involved in almost every facet of Colombian society, but perhaps nowhere more significantly than in supporting local farmers who grow coca throughout the Andean region. Coca farmers only see about one percent of the profit made from cocaine. However, this amounts to several thousand dollars each year, between 10 and 100 times more than they could earn from any legal crop.[59] The cartels make the farmer's decision whether to grow coca or legal crops even easier by the incentives they provide. Cartels will provide farmers everything they need to begin growing coca including financing, seed, and technical assistance. They will pick up the

[57] MacDonald, 1989, 24.
[58] Ibid., 35.
[59] Filippone, 1994, 329.

finished product, instead of making the farmers transport their crops. Also, the cartels provide protection through intimidation or bribes of local authorities.[60]

All this, combined with the long history of legal coca cultivation in Latin America, gives farmers all the incentive they need to grow coca on as much land as they can. The government has offered to assist farmers' transition to other crops, but there is little financial incentive to do so. So the Colombian government, decertified in 1996 from receiving U.S. economic aid because of being too weak on drugs, has vowed to wipe out the crops with police help. In August 1996, over 30,000 Colombian farmers turned out to protest the government's move. These farmers blocked roads and airstrips to prevent defoliant-spraying aircraft and trucks from destroying their crops. Protesters have even retaliated by blowing up a section of an oil pipeline.[61]

There is at least one significant difference between the old Colombian cartels and the new ones that have emerged. Where the Colombian cartel leaders sought to be recognized as "pillars of society", the new cartels have shown no apparent interest in anything but financial gain. Similarly, while the Colombian cartels employ numerous farmers and additional help for cocaine production, the Mexican cartels mainly transport the finished cocaine, providing far fewer opportunities to provide work for poor Mexicans. It is entirely possible that the new cartels will lose the popular support they once had in some parts of society.

[60] Ibid., 329.

[61] "Coca Clashes," The Economist, 17 August 1996, 35.

Finally, Mexico's proximity to the United States has enabled the cartels to join with U.S. gangs and drug dealers. Mexican drug trade crosses borders into the United States as easily as Colombia's trade with Peru and Bolivia. Mexican cartels recruit from U.S. cities, and methamphetamine production by Mexican drug traffickers takes place on both sides of the border. Due to the borderless nature of the drug cartels, dealers and criminals from both nations use the border to hide from prosecution. This makes Mexican cartels even more threatening to U.S. security than previous cartels were. According to one U.S. law enforcement official, "Unlike Colombia, the Mexicans have the ability to carry the violence across the border."[62]

d. *Innovation*

One effect of the loose, network structure is that the drug cartels have been particularly innovative in their methods of processing and transportation. When government officials appear to make gains in one area of coca growth or processing, the cartels simply move their operations into areas where the government does not have control. When interdiction efforts successfully cut off a supply route, smugglers move to other routes that take advantage of legal and geographic gray-areas. According to one author, "drug producers, traffickers, and consumers alike have all been able to exploit the limited ability of states to control what happens within their borders and what passes across them."[63]

[62] Anne-Marie O'Connor, "U.S. Fears Escalation of Mexico's Drug Violence," The Los Angeles Times, 22 September 1996.
[63] Stares, 1996, 46.

For example, in 1995 the United States, Colombian, and Peruvian governments targeted the "air bridge" used to transport coca paste from Peru to Colombia. The goal was to stop the supply of raw materials into Colombia by following and forcing down drug-smuggling aircraft. The operation was quite a feat considering Peruvian and Colombian aircraft had to coordinate operations in order to hand off the aircraft as they crossed international borders. This operation was fairly successful (with over 35 drug-smuggling planes forced or shot down)[64] until the drug planes changed their route to fly over Brazil, whose government refused to participate in air-interdiction efforts.

Almost weekly there are reports of drugs being smuggled into the United States through every means imaginable. For example, according to the U.S. Department of Justice, a courier had a half pound of cocaine surgically implanted under the skin of each of his thighs; more than a ton of drugs were carried through a 30-foot deep, concrete-reinforced tunnel that ran under the U.S.-Mexican border; cocaine was wrapped in small plastic packets and buried inside 55-gallon drums of a toxic powdered chemical; a shipment containing 25 boxes of live goldfish included dead fish which had been loaded with 3 pounds of heroin; Panamanian cocaine smugglers developed a new technology that combines cocaine with vinyl to produce a material that has been used in making luggage and sneakers (the cocaine is separated from the vinyl after reaching its destination.)[65] More recently, in February 1997 the DEA arrested an Israeli arms dealer in Florida who

[64] DEA Intelligence Bulletin, The South American Cocaine Trade: An Industry in Transition, 1 July 1996, 3.
[65] Drugs, Crime, and the Justice System, 1992, 44-45.

was operating as a middleman for a Colombian cartel trying to purchase a Russian nuclear-powered submarine.[66] Due to the huge amounts of profit in drug smuggling, there are great incentives to use innovative means to transport marijuana, cocaine and heroin. Even if some of the drugs are periodically discovered and captured, the payoff is great for those who avoid detection.

The cartels have even introduced innovative product ideas. The Cali cartel, realizing that they were limiting their market to the wealthy population of drug users in the United States, developed crack cocaine as a low-cost drug for those too poor to buy cocaine.[67] Both the decentralized nature of the drug business, and the huge rewards for those who use creative means to avoid detection, favor innovation. Similarly, since the mid-1990's the Colombian cartels have grown and marketed a type of heroin that is many times more pure than Asian heroin, yet it is sold at a fraction of the price.

The cartel's greatest innovation, however, was the organizational decision to combine operations and coordinate activities. The U.S. national security structure has reacted to many of the new tactics and techniques of the drug cartels. But the organizational shift that the cartels made was apparently not matched by the United States' counternarcotics forces.

[66] "U.S. Says Drug Smugglers Tried to Buy Sub," Reuters news wire, 7 February 1997.
[67] Kerry, 1997, 88.

B. RESPONSE

> There are no impossible situations. There are only people who think they're impossible.
>
> President Reagan, quoting a French soldier at the Battle of Verdun, after declaring the "War on Drugs".[68]

1. History of the Drug War

The United States' response to the threat of illegal drugs was the "War on Drugs". Although this catchy phrase was introduced by President Reagan in 1981, efforts to stem the flow of illegal drugs into the United States began in earnest during the Vietnam War. Candidates running in the 1968 presidential election needed a campaign issue that would divert attention away from war in Vietnam. The issue they chose was illegal drug use in America. According to then-candidate Richard Nixon, the nation's attitude of lawlessness and rebellion was fueled by illegal drugs. In a campaign speech given at Disneyland, Nixon stated, "As I look over the problems in this country, I see one that stands out particularly. The problem of narcotics."[69] He set about creating an anti-crime campaign that would triple the size of the Customs Service and increase aid to federal and local police forces.

Still, drug use in America continued to grow. Nixon's anti-drug campaign, for a variety of reasons, was neither successful in stemming the supply of nor the demand for drugs. President Carter continued Nixon's offensive, but with similarly poor results. In

[68] Dan Baum, Smoke and Mirrors, New York: Little, Brown and Co., 1996, 165.
[69] Ibid., 12.

1981, shortly after taking office, President Reagan escalated the fight against drug use by declaring a "War on Drugs". In addition to tasking the FBI to counter drugs in America, President Reagan decided to formally task the military with supporting counternarcotics operations. Although the military had been used to support counternarcotics operations periodically in the past, President Reagan officially amended the Posse Comitatus Act[70] in 1982 in order to formalize the military's role in the drug war.[71] Ordered by the National Defense Authorization Act of 1989, and then passed into law by Title 10 of the U.S. Code, the military was tasked to take the lead in the detection and monitoring of illegal drug shipments into the United States. Drugs, because of the negative effects they had on society, were officially declared a threat to the security of the United States.

Even though more and more organizations were being tasked with participating in the Drug War, there was little strategic guidance or coordination. As a result, Congress passed the federal Anti-Drug Abuse Act of 1988. This act established the Office of National Drug Control Policy which set objectives for national drug control. Long-term strategy was communicated with the annual *National Drug Control Strategy* which supposedly guides efforts of all involved organizations.[72] But the Office of National Drug Control Policy was established as a policy-making office, with no operational control over any counterdrug assets. Efforts to counter the import and use of drugs continue today, however the amount of drugs coming into the United States and the profits associated

[70] The Posse Comitatus Act was passed in 1876 to prevent U.S. military forces from conducting law enforcement functions against American citizens.

[71] Baum, 1996, 167.

[72] Office of National Drug Control Policy, 1997 National Drug Control Strategy, , Washington DC, February 1997.

with narcotics production and trafficking have increased while the price of drugs has gone down or remained the same. Although there may be several reasons for the ineffectiveness of U.S. efforts, the organizational structure used to fight the drug traffickers is almost certainly one factor in the failure to counter drug sales in the United States.

2. Multi-Agency, Multi-National Structure

Unlike the drug cartels, which have spent the past 15 years improving coordination, the national security establishment responsible for stemming the flow of illegal drugs into America has become increasingly fractured. According to the 1997 National Drug Control Strategy, "In order for demand and supply initiatives to work, they must be supported by appropriate organizational structures... and intergovernmental (federal, state, and local) coordination."[73] Due to the bureaucratic nature of federal and state government organizations, this has proved to be extremely difficult .

a. *Command and Control*

There are over 35 federal organizations that are responsible for participating in counterdrug operations. Additionally, there are countless state and local level organizations that are tasked with stemming the flow of drugs into the United States. Although the U.S. military and national intelligence agencies are tasked with monitoring and detection of drug smuggling, the law enforcement organizations are ultimately held responsible for arresting drug traffickers and stopping the flow of drugs into the United States. This division of roles complicates arrests and prosecution, and requires a high

[73] Ibid., 32.

level of interaction between the many different offices involved in international and domestic counternarcotics operations.

For the most part, all of these organizations are part of the bureaucratic system that makes up our national security structure. These organizations have different cultures and strategies, making it difficult to communicate and coordinate across organizational lines. The emphasis on command and control differs between law enforcement and military organizations. Where the military works on a top-down, hierarchical structure, law enforcement operates along more ad hoc lines. For example, when a commanding officer in a military unit is removed, command falls down one level in the chain-of-command. When a law enforcement commander is removed, command moves up one level.[74] Also, the law enforcement hierarchy is more fluid than that of the military or intelligence services. Law enforcement personnel are assigned cases, and where one officer may support another on a raid one day, he may be leading his co-workers on a raid the next. Another cultural difference between military and law enforcement personnel is that military personnel are trained to make quick and decisive decisions, while law enforcement personnel, especially in multi-jurisdictional operations, rule by consensus.[75] Issues such as these make coordination between law enforcement and military support organizations difficult, and cultural clashes can lead to bad feelings on both sides.

[74] Christopher Schnaubelt, "Interagency Command and Control: Planning for Counterdrug Support," Military Review, September-October 1996, 21.
[75] Ibid., 22.

Some of these problems of coordination have been addressed, but not solved, in the formation of three Joint Interagency Task Forces (discussed below), tasked with providing command and control for the military and law enforcement assets assigned to interdiction.

b. *Intelligence*

There are two different "types" of intelligence used in counternarcotics. First, national level agencies (Central Intelligence Agency, National Reconnaissance Office, State Department) and military intelligence agencies (Defense Intelligence Agency, service intelligence organizations) focus on collecting information on cartel leaders, production capabilities, and smuggling routes. The law enforcement community (Federal Bureau of Investigation, Drug Enforcement Administration, Customs) also collects intelligence on the U.S. side of the drug trafficking network.

Like the military and law enforcement agencies, the national intelligence services are organized hierarchically. In addition to the strict organizational hierarchy that exists in the federal government, there also exists bureaucracy in the form of classification where certain information cannot be passed on to personnel without the proper security clearances and a "need to know." The national intelligence agencies must often protect their sources, but in doing so may hold back bits of information that would reveal the source of that information. According to Joint Pub 3-07.4, Joint Counterdrug Operations, "To protect DOD sources and methods from unauthorized disclosure, certain sensitive compartmented information and sensitive human intelligence information is either not released or is sanitized and the classification downgraded to make the information usable outside the Intelligence Community."[76] This has led to inter-agency rivalry where organizations withhold information that could be used to convict drug lords who are later set free.

Law enforcement, including DEA, FBI, and state and local police forces, also collect intelligence. They attempt to break up drug networks in the United States by infiltrating the organization or "turning" informants. The purpose is to arrest dealers at the highest level possible, and prevent the dispersal of drugs to smaller dealers. However, collecting intelligence on drug cartels has proven to be difficult for a variety of reasons. The drug cartels are highly integrated, and loyalty to the organization is virtually guaranteed both because of the huge sums of money paid out, and because of the incredibly violent means the organization uses to punish traitors. Due to the compartmented flow of information at this level of the drug network, lower level dealers often have little useful information about their foreign connections. Also, the number of people willing to become involved in the drug trade guarantees the position will be filled again to meet the demand.

Intelligence sharing can be difficult at the local level as well. Law enforcement intelligence is done locally, with no formal structure to pass on information. Law enforcement intelligence, in fact, is closer to a network structure than any other part of the counternarcotics structure, and the U.S. intelligence services may find it helpful to

[76] Department of Defense, Joint Pub 3-07.4, Joint Counterdrug Operations, Washington DC, August 1994, IV-24.

emulate their structure. Information is passed laterally and informally to anyone who may need the information. But another part of the system may discourage passing certain types of information. Since police forces are given assets seized during drug raids, there may be little incentive to pass intelligence information to other agencies. For example, intelligence developed in San Diego about a drug deal occurring in Los Angeles may not be passed on if it is believed the traffickers will be returning to San Diego with their profits. With the huge sums of money and high-tech equipment involved, seizures can make up a significant part of a local police force's counternarcotics budget.

Even more challenging is the international dimension of intelligence sharing. Intelligence collected by the United States is often difficult to pass to foreign nationals, and limitations on U.S. intelligence collection often prevents information from being collected and utilized. According to DEA Administrator Thomas Constantine, "There has been limited sharing of intelligence information between U.S. and Mexican law enforcement agencies due to the lack of an appropriate infrastructure. The DEA often cannot receive tactical intelligence from these law enforcement counterparts due to their inability to collect such information."[77]

c. *Alliances*

The United States works with many other nations to combat the production and transport of illegal drugs. However, these alliances are often strained and run into strict limitations. The United States' two main allies in the drug war have

[77] Drug Trafficking in Mexico, 1996, 6.

historically been Colombia and Mexico. Both countries have recognized the impact that drug cartels have had on their governments and have historically worked closely with the United States tracking and arresting cartel leaders. However, every year the United States reviews the contributions of these countries and determines whether they have "done enough" in combating drugs. In 1996, Colombia was decertified by the United States as not being supportive enough, and Mexico almost suffered a similar fate in February 1997 when the U.S. congress attempted to pass legislation overturning President Clinton's certification of Mexico.[78]

The certification process, combined with Latin America's historic fear of U.S. domination, have led to resistance in Latin American governments to embrace multi-national counternarcotics operations. One author points out that, "[n]arcotics lobbies consistently equate drug control with a loss of national sovereignty; and leftist intellectuals see it as reinforcing U.S. domination of Latin America's political, military, and public institutions."[79] The United States reaction to this has been to use economic and political pressure to force Latin American governments into compliance. However, this only strengthens the impression that the United States is acting in its own self interests.

d. *Innovation*

The United States has innovated little in the Drug War. The two main strategies have been to prevent drugs from reaching the United States (countering supply), and to reduce demand for drugs in the United States. Attacking the supply of drugs has

[78] Peter Slevin, "House Panel Wants Mexico Decertified," Miami Herald, 7 March 97.
[79] Lee, 1990, 196.

wavered between interdicting drugs as they are smuggled from Latin America into the United States, and stopping drugs at the source through crop substitution and eradication efforts. But the U.S. national security structure has been largely predictable when it comes to counternarcotics operations. Law enforcement personnel have been flexible enough to discover drug shipments smuggled in virtually everything possible, but the smugglers have the advantage when it comes to innovation. While counternarcotics organizations are attempting to use technology to assist in their jobs (drug sniffing devices are being developed to replace dogs at the borders), the limited number of U.S. officials combined with the huge volume of traffic crossing the borders daily practically guarantees well-hidden caches of drugs will make it across the border undetected.

Innovation in the federal government is stifled by numerous procedures and bureaucratization. Similarly, the risks involved in innovation prevent counternarcotics organizations from embracing unproved ideas. As long as law enforcement agencies can show an increase in the amount of drugs confiscated, or the government can show a decrease in drug consumption, there is little incentive to make dramatic changes in operations.

C. RESULT

By any measure (the amount of illegal drugs flowing into the United States, the street price of drugs, the profits involved with selling drugs, etc.), the United States has not been effective in stopping either the flow of drugs into the United States or the demand for illegal drugs. This is not to say the drug cartels operate with complete impunity. But the United States' goal of countering the flow of narcotics into the United States has not been achieved, while the cartels' goal of making profit has been achieved to a very high degree. In 1997, President Clinton effectively declared an end to the "War on Drugs". Instead of being a "war", the Clinton administration likens the U.S.' drug problem to a "cancer" that must be dealt with in the long-term.[80]

It should be noted that the United States has made some improvements to the way it has conducted counternarcotics operations in recent years. For example, the formation of several Joint Interagency Task Forces (JIATF)—collections of law enforcement, military, and intelligence officials geographically co-located—in 1994 may show a growing realization of the importance of integrated action. JIATF East, located in Key West, Florida, brings together 180 representatives from the four military services, the Coast Guard, and the U.S. Customs Service who act as coordinators for joint-interagency counterdrug operations. However, it is unclear how much the new JIATF organization resembles the bureaucratic organizations of old, or how effective JIATF personnel can be when their parent organizations are still reluctant to share information and resources. Despite the appearance of being a decentralized organization, one intelligence official points out that JIATF East organizationally falls under US Atlantic Command (a combatant command of the Department of Defense) and therefore does not enjoy the flexibility required to counter the agile drug cartels.[81]

[80] Angie Cannon, "$16 billion drug plan emphasizes ads, courts", Miami Herald, 26 February 1997.
[81] Interview with an intelligence official with ten years experience in counternarcotics operations. He prefers his name not be used in this thesis.

Comparing the cartel structure to the counternarcotics structure that has formed to counter the production and sale of illegal drugs, it is clear that organizational structure reduces U.S. effectiveness in countering drugs.

	Command and Control	Intelligence	Alliances	Innovation
Latin American Drug Cartels	Strategic core Decentralized operations	High-tech equipment Corruption	Guerrillas Government Mass Public TCOs	Very innovative at all levels Innovation is rewarded
U.S. National Security Structure	Highly bureaucratic Multi-organizational involvement	Centralized and compartmented Intelligence-sharing difficult	Fragile and subject to politics	Low innovation No incentive to innovate

Table 4.1: Comparison of Latin American Drug Cartels to U.S. Security Structure

Where the drug cartels have created a "seamless" organization, with free-flowing communications and decentralized decision making, the United States has created a bureaucracy subject to compartmentalized information flow and organizational conflict. As a result, the drug cartels have consistently outperformed the organizations created to counter them. Decentralized decision making and constant communications enables drug cartels to collect and pass information quicker than U.S. counternarcotics organizations. It has also enabled members of the drug cartels to be more innovative than U.S. law enforcement and military personnel.

It is also clear that the drug cartels are aware of the importance of organizational design on their success. Following his arrest for drug corruption in March 1997, Mexican Army General Alfredo Navarro Lara stated that the Tijuana cartel was "perfectly structured and organized, and that they (authorities) wouldn't be able to deter them because they have support both in the United States and Mexico."[82] Even some the United States government have realized that the United States is not properly organized to fight drugs. FBI Director Louis Freeh sent a memo to President Clinton in October 1996 stating, "(t)he federal government had never been properly organized in terms of who had jurisdiction to do what in the drug war."[83]

But recognizing the problem and solving the problem are two different things. As shown in the previous chapter, it will prove to be extremely difficult for the bureaucracy to change without external pressures placed upon it, and without making significant changes in its culture. One attribute of bureaucracy is that it is inherently resistant to change. Still, unless the United States adopts at least some attributes of a network structure, the drug cartels will continue to outperform efforts to stop the production and transit of illegal drugs. The U.S. bureaucracy limits flexibility and inhibits innovation of the sorts that exist and arise in the networked drug cartels. Additionally, the United States must be willing to work with Latin American governments to reduce their bureaucracy as well. The drug problem may be considered a threat to U.S. security, but there is obviously no unilateral solution. Despite cumbersome laws that separate the task of international and domestic

[82] "Mexico General Faces Bribe Case," Associated Press, 18 March 1997.
[83] "Clinton Says Secret Memo Finds War on Drugs Organization Lacking," Associated Press, 4 October 1996.

law enforcement, the nature of the drug trade requires a networked response free of such barriers. Even Administrator Constantine recognizes that, "[i]n truth, the global drug trade is a seamless continuum, with no clear lines of demarcation between international and domestic drug trafficking."[84] A counternarcotics network, made up of U.S. and foreign military, intelligence, and law enforcement officials, would be the most effective way to attack the drug cartels.

[84] DEA Congressional Testimony, National Drug Control Strategy and Drug Interdiction, 12 September 1996, 2.

IV. NEW CHALLENGES OF THE INFORMATION AGE

> The world is in the midst of an extended post-Cold War transition that will last at least another decade.
>
> Lt. Gen. Patrick Hughes
> Director, Defense Intelligence Agency[1]

A. THE RISE OF ENVIRONMENTAL UNCERTAINTY

The rise of the Information Age has led to a world that bears little resemblance to that of the past fifty years. The world is now in a period of revolutionary change in which national security has become increasingly challenging and uncertain. Instead of seeing an era of peaceful coexistence, the end of the Cold War and the rise of the Information Age has led to a security environment that is neither predictable nor static. Unlike the Cold War era, threats in the Information Age can emerge almost without warning and often defy a traditional military response. The national security structure, like many businesses, has found that its operating environment has changed dramatically.

1. End of the Cold War

The national security threat during the Cold War was easily identifiable and largely static. The threat posed by the Soviet Union gave the national security structure a single threat on which to focus its efforts. Although there were threats from other nation-states, the bipolar nature of conflict linked most threats to U.S. security back to the Soviet Union. The national security structure that exists today was designed to counter this singular threat. During the Cold war the United States organized, trained, and equipped

[1] Cited in Rick Maze, "Few Threats are Predicted," Air Force Times, 17 February 1997.

huge numbers of maneuverable forces and pre-positioned them throughout the globe to react to any threat to the United States or its allies. Forces maintained a high state of readiness in places, such as the Fulda Gap, where the Soviet Union was expected to attack. A formula of indications and warnings were developed to detect impending attack or hostilities. Military commanders designed and maintained volumes of war plans created under the "deliberate planning process"[2] that sought to predict where attacks would occur and plan for a standardized response.

Long-term planning was essential to Cold War readiness. Strategic planning was conducted with an eye towards maintaining a global balance of power. Models and simulations allowed planners to determine what the right mix of equipment and forces were in order to counter the threat posed by Soviet forces. Intelligence collection helped determine what systems the Soviets were building so the U.S. could counter them with its own systems. Intelligence analysis focused on numbers and placement of equipment, or order-of-battle, to determine the strong and weak points of the adversary.

This huge, bureaucratic national security structure operated for a half-century in this manner. The threat was long-term, and it was largely static because changes came slowly and were often predictable. The U.S. faced a known, and relatively undynamic, security environment that allowed it to conduct long-term planning and acquisition strategies. Each part of the organization knew exactly how to react to the limited number

[2] According to Joint Pub 5-0, Doctrine for Planning Joint Operations, deliberate planning is defined as "a planning process for the deployment and employment of apportioned forces and resources that occurs in response to a hypothetical situation. Deliberate planners rely heavily on assumptions regarding the circumstances that will exist when the plan is executed."

of scenarios possible, and efficiency was maintained through standardized doctrine and training exercises. The military-industrial complex was literally a machine working towards one specific goal: containment of communism around the world.

The end of the Cold War had a dramatic impact on global security. The collapse of the Soviet Union, and the virtual disappearance of the communist threat, has left the U.S. without a "peer competitor" that poses a tangible threat to U.S. national security. The change from a bipolar to multipolar world[3] has not resulted in the expected "end of History".[4] Rather, the world faces a more diverse range of threats than ever, including ethnic conflict, the proliferation of weapons of mass destruction, terrorism, transnational crime, and drug trafficking[5]. While the U.S. security structure focused on one main threat during the Cold War, it is now being forced to maintain a global focus to counter threats from any number of state and non-state actors.

Despite the widening nature of the threat, the top U.S. leadership are still debating the shape of the future security structure. Many U.S. policy-makers question the necessity of a large standing military in a post-Cold War environment, saying improved intelligence collection and Precision Guided Munitions will make mass armies a thing of the past. Others speculate that the U.S. could face another peer competitor, most likely China, in

[3] Multipolar not in regards to the existence of many great powers, but rather the general absence of any dominant power. See footnote #2 in Chapter I regarding Keohane and Nye's "theory of complex interdependence".
[4] Francis Fukuyama wrote an article entitled "The end of History?" (The National Interest, Summer 1989, 3-18) in which he posited that the death of communism in Eastern Europe would result in western liberal democracy predominating in the world. This, he concluded, would mean the end of war, pointing to the Kantian notion that democracies don't go to war with each other.
[5] Threats identified in A National Security Strategy for a New Century, Executive Office of the President, Washington, DC, May 1997.

the next ten years which requires keeping the military-industrial complex intact. Because of this, they maintain, the U.S. should continue down the same path it took during the Cold War—using large numbers of advanced equipment and troops—in order to remain competitive in the next century.

In the meantime, the military is being called on to perform more and more "non-traditional" missions because of its unique training and equipment. Despite the lack of a peer competitor, operations tempo for military forces seems to be higher than ever. New threats such as the proliferation of weapons of mass destruction and transnational crime, and older threats such as narcotics trafficking and terrorism, have taken on new precedence as security challenges of the post-Cold War era. The U.S. national security strategy of containment has been replaced by a rather vague one of "engagement and enlargement".

2. Rise of the Information Age

The end of the Cold War, in itself, did not create the uncertain security environment that exists today. Without the threat of the Soviet Union, the United States may have seen the much-anticipated "peace dividend." At the very least, the national security structure would have shifted its intense focus to another superpower candidate like China. However, at the same time the Berlin Wall was crumbling and the Communist regime was failing, another phenomenon was occurring on a global scale: the Information Revolution.

Dramatic advances in computer processing and telecommunications technology have led to unprecedented information storage, processing, and transfer capabilities. Advances in information technology are occurring at an increasingly rapid pace, and worldwide connectivity is quickly becoming a reality. The impact of computers, modems, satellite communications, and cryptography is only beginning to affect our lives.[6]

The world is, depending on who you listen to, either on the verge of or in the middle of the Information Age. The rapid rise of technology has pushed the United States, and other developed countries, into what futurist Alvin Toffler calls the "Third Wave";[7] the First Wave being the agricultural revolution, the Second Wave the Industrial Revolution, and the Third Wave the Information Revolution. His argument is that the way countries make wealth is reflected in the way they make war, and thus war in the Information Age will rely largely on the collection and processing of vast amounts of information.

Much of the change in the national security environment can be attributed to the Information Revolution, giving previously inefficient groups the capability to communicate and attack in greater secrecy and ambiguity.

3. The World Today

It is clear that there exists a significantly different security environment today than there was ten years ago. On the one hand, the overall threat to U.S. security has

[6] For a thought-provoking view of the changes we will face in the Information Age, see Nicholas Negroponte's Being Digital (New York: Vintage Books, 1995.)

[7] Alvin Toffler, The Third Wave, New York: Bantam Books, 1980. Alvin & Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century, New York: Little Brown and Co., 1993.

diminished with the collapse of the Soviet Union and the dismantling of many weapons-of-mass-destruction. On the other hand, the spectrum of threats has vastly increased with the end of the two-superpower struggle.

Complicating matters is that it is as yet unclear what type of threat will predominate in the future world, or if there will even be a "dominant" threat. Based on the findings of the 1997 Quadrennial Defense Review (QDR), the U.S. military is still planning on fighting large, hierarchical military forces.[8] At the same time, the QDR calls for purchases of the latest information technology to exploit the "Revolution in Military Affairs." It is argued that information technology will allow the U.S. to operate quicker and more accurately against lesser-developed military forces.

However, we have seen that the world will also include lesser threats that may not operate in traditional ways. The military has always been faced with a wide "spectrum of conflict", from low-intensity conflict to global war. But the Information Age is providing an even wider spectrum of conflict than ever, including an almost constant threat from any number of groups (hackers, cyberspies, transnational criminal organizations, etc.) For the first time, the U.S. military, working in concert with law enforcement agencies and intelligence organizations, will face constant challenges to U.S. national security on its own territory.

A 1979 novel written by science fiction author Frederick Pohl entitled The Cool War[9] describes a future world in which war was banned following the destruction of the

[8] The QDR calls for a force capable of handling two major regional contingencies in different parts of the world.

[9] Frederik Pohl, The Cool War, New York: Ballantine Books, 1979.

world's oil supply in the Middle East. Although the traditional notion of war doesn't exist, nations continue to battle at a much lower level of conflict. Government agents input virulent strains of the flu into its adversary's work force, leading to decreased production of resources. Covert agents sabotage power supplies so that power failures become a regular occurrence. Revolutionary sympathizers in drought areas run their taps all day and turn on fire hydrants. As one of the characters puts it, "War is not all bombs and missiles.... It's hurting the other fellow any way you can. And if you can hurt him so he can't prove it's happening, why, that's one for your side."[10] These menacing actions are not considered "warfare," and many are not even identified as intentional acts. However they are constant threats—or at least annoyances—that impact society's overall quality of life. Like Pohl's Cool War, the Information Age will likely consist of constant, but minor, threats to U.S. national security, some of which we won't even recognize as attacks.

In the post-Cold War era, national security does not just mean the U.S. faces military threats. Nor does it mean that losing a "war" against its competitor will lead to the downfall of the U.S. government. Whereas the traditional goal of warfare has been to overthrow an existing government, new threats often seek to maintain status quo or even completely bypass governments. Transnational criminal organizations often choose to operate out of weak states to avoid legal persecution and harsh punishments. Rather than overthrowing the government that provides them security, these organizations seek to

[10] Ibid., 21.

maintain the weak or corrupt government. For example, the Colombian drug cartels have supported a variety of high-level politicians, including the Colombian President Ernesto Samper.[11] Similarly, the Russian Mafyia surged in growth following the collapse of the oppressive Soviet regime and thrives under the more lenient, and disorganized, democratic government of today.[12] One problem, however, is that these criminal organizations also oppose strengthening these governments, and attempt to subvert democratic consolidation that is favorable to regional stability.

Another significant trend in the Information Age has been the blending of foreign and domestic threats. The distinctions between threats from outside the United States' borders and from inside its borders have begun to blur. For example, the much-feared cyber attack against the U.S. information infrastructure could emerge from outside or inside U.S. borders while appearing to come from somewhere else entirely. Yet the hierarchical structure of the national security organizations has imposed strict rules regarding operations against foreign or domestic targets. Similarly, the lines between challenges to U.S. national security and simple criminal activity have been blurred. The proliferation of weapons of mass destruction are an example of transnational criminal activity with significant consequences to U.S. national security. This, too, transcends the boundaries built by the U.S. bureaucracy to divide responsibility for law enforcement and military activity.

[11] Karsten Prager, "Drugs, Money and a President's Ruin," Time, 5 February 1996, 37. "Colombia Arrests Senator on Drug Corruption Charges," The Orlando Sentinel, 25 April 1996, A12.
[12] Kerry, 1997, 34.

The Information Age has also brought with it a new group of threats that have either emerged from previous groups or formed in response to changes in the world security environment. Arms traffickers have always illegally bought and sold weaponry to rogue nations, but today the world is faced with the threat of nuclear, biological, and chemical agents being sold to rogue nations, and possibly even non-nation state organizations. Computer "hackers" have also been around ever since the birth of the personal computer, but where the original hackers prided themselves on merely "looking around,"[13] today's hackers develop computer viruses, download sensitive data, and steal millions of dollars[14]. Not surprisingly, there are already reports that drug cartels and other organized criminal groups have hired hackers for a variety of purposes. According to one article, "Hackers can get into court computer systems and find out about wiretaps and then sell that information to the people who have been tapped. Then they offer to get rid of the tap too."[15]

4. The Advent of Netwar

As previously discussed, the drug cartels have emerged as a networked threat of the Information Age. There are, however, numerous other threats that are following the

[13] The book Masters of Deception (Michelle Slatalla and Joshua Quittner, Masters of Deception: The Gang That Ruled Cyberspace, New York: Harper Collins Publishers, 1995) gives a good description of various hacker groups, their capabilities, and the "Hacker Ethic" of not causing any harm.

[14] According to an article in 1995 (John Mason, "Russian 'in $2.8m Citibank computer fraud,'" Financial Times, 18 August 1995) a Russian computer hacker was able to transfer almost three million dollars into his account by accessing Citibank's Wall Street computer. The transfer was detected and the hacker was arrested in England where he awaits extradition to the U.S.

[15] Bob Brewin and Elizabeth Sikorovsky, "Hackers Storm DOD Nets," Federal Computer Week, 11 July 1994, 4.

same path as the cartels. John Arquilla and David Ronfeldt[16] identify emerging threats of the Information Age and predict a new war-form that takes advantage of advancing technology and the increasingly "borderless" nature of the world. Arquilla and Ronfeldt differentiate between "cyberwar", which they define as "knowledge-related conflict at the military level," and "netwar" which involves "societal struggles most often associated with low intensity conflict by non-state actors, such as terrorists, drug cartels, or black market proliferators of weapons of mass destruction."[17] While cyberwar mainly applies new technologies and capabilities to the existing concept of modern warfare, one of large militaries facing each other in battle, netwar predicts an entirely new form of warfare in which organizational structure plays a significant role.

Subsequent to their first article, Arquilla and Ronfeldt published a study in 1996 for RAND's National Defense Research Institute entitled "The Advent of Netwar" which expands on the notion of netwar. According to their theory of netwar, non-state threats like drug cartels, terrorist organizations, and weapons proliferators now rely on the network form of organization. "These protagonists generally consist of dispersed, often small groups who agree to communicate, coordinate, and act in an internetted manner, often without a precise central leadership or headquarters."[18] These networked organizations have several distinguishing characteristics that make them different from

[16] John Arquilla and David Ronfeldt, "Cyberwar is coming!", Comparative Strategy, Volume 12, no. 2, 1993, 141-165.

[17] Ibid.

[18] John Arquilla and David Ronfeldt, "The Advent of Netwar," Santa Monica, CA: RAND, 1996, 5.

other types of organizations: they consist of dispersed, but interconnected, "nodes"[19]; they have a flat structure, with no central command and very little hierarchy; they have a centralized doctrine, but are operationally decentralized; and there is a large amount of communication between different parts of the organization.

Netwar threats exist at all levels, from subnational to transnational, and have varying relations with state actors. According to Arquilla and Ronfeldt, all netwar threats share the network form of organization, doctrine, strategy, and communication that take advantage of the technological advances of the Information Age. The authors point out that there have been many examples of netwar-like groups in the past[20]—often classified as low-intensity conflict or operations-other-than-war or criminal activity—but the high amount of communication required to make a networked organization effective did not exist until recently. These emerging netwar threats are, for the first time, intentionally choosing the network form of organization and are able to maintain contact over great distances and long periods of time. Although the authors feel the phenomenon of netwar is still emerging, they predict netwar will be the more likely, and more challenging, form of conflict in the Information Age.

It is possible to make some general predictions about the new threats of the Information Age by reviewing Arquilla and Ronfeldt's theory of netwar, and then looking

[19] Nodes can be large or small and are made up of individuals, groups, organizations, or parts of organizations.

[20] Their list includes irregular warfare in North America during the French and Indian Wars and the American Revolution, Spanish guerrillas operating against the Napoleonic occupation in the early nineteenth century; and pirates, terrorists, and various other criminal groups. According to Arquilla and Ronfeldt, all these groups "have long operated on the fringes of empires and nation-states."

at current events to see if there are any indications that netwar is becoming reality. This section is not intended to be a longitudinal study of headlines over a set period of time to determine if there are more articles supporting the theory of netwar than there are articles disproving it. Rather, it is intended to show that we can already see manifestations of our future security environment in today's headlines. Like Plato's cave,[21] we can see shadows on the wall that loosely represent the shape of our future security environment. Through its review of organization theory and the theory of netwar, this study will hopefully bring some of these current events into focus so we are not confused when faced with the reality of tomorrow's security challenges.

For purposes of comparison, it is beneficial to look at the threat of netwar using the same template that was used to evaluate the drug war, and then compare this to the structure being created by the U.S. to counter these Information Age threats.

a. Command and Control

As already indicated, netwar actors use the network form of organization. Inherent in this form is the decentralization of command and control at all levels. "There is no single central leader or commander; the network as a whole (but not necessarily each node) has little or no hierarchy. There may be multiple leaders. Decision making and

[21] An allegory used in Plato's Republic describes a group of prisoners who are held in a cave with their backs to the light at the mouth of the cave. The prisoners only see objects as shadows reflected on the walls of the cave. When the prisoners are eventually let out, they are confused by the clarity of the actual objects. But over time the prisoners become accustomed to seeing the objects as they truly appear. When brought back to the cave the liberated prisoners see the shadows are only distortions of reality, but the remaining prisoners are disturbed by those who challenge everything they know as "real."

operations are decentralized and depend on consultative consensus-building that allows for local initiative and autonomy."[22]

Unlike hierarchical organizations which require regulations and constant direction for effective operations, netwar organizations are able to perform effectively through a shared sense of purpose. "Such a doctrine can enable them to be 'all of one mind' even if they are dispersed and devoted to different tasks. It can prove ideational, strategic, and operational centrality that allows for tactical decentralization. It can set boundaries and provide guidelines for decisions and actions so that they do not have to resort to a hierarchy...."[23]

Aside from the drug cartels, other types of groups have shown a trend towards a network structure. Many groups take advantage of computer networks—mainly the Internet—to coordinate and gain support. Mexico's Zapatista guerrilla group has taken advantage of computer technology to coordinate their activities, circumvent the government-controlled media, and link widely-distributed support groups throughout the region and the world.[24] By placing their "Manifesto" on-line, the Zapatistas are able to spread their doctrine and give strategic guidance to aspiring revolutionaries all over the globe. Similarly, combatants on all sides of the conflict in the Former Yugoslavia have

[22] Arquilla and Ronfeldt, 1996, 9.

[23] Ibid., 10.

[24] Harry Cleaver, "The Zapatistas and the Electronic Fabric of Struggle," 1995, Internet: www.eco.utexas.edu/homepages/faculty/Cleaver/zaps.html.

used the Internet to wage an "information war" that is every bit as complex as the fighting on the ground.[25]

Mirroring the structural change the drug cartels underwent in the 1980s, many criminal groups are modifying their structures to look less like hierarchies and more like networks. Terrorist organizations, both foreign and domestic, have always used decentralization to conduct operations and increase secrecy. But new information technologies, like publicly available cryptography, secure telecommunications, and anonymous e-mail, have given them increased coordination capability with even lesser risk to the organization. Where the decentralized, but compartmented, "cell" structure of old terrorist and criminal groups was an operational necessity, networked groups are able to communicate in secret, with less risk of exposure from infiltrators or captured members.

The key to effective network organizations is modern communications technology that is allowing dispersed members of the organization to be in constant communication. Although criminal groups cannot always operate overtly—the illegal nature of their business permits law enforcement agencies to intercept communications and use the information gathered as evidence—today's technologies allow greater and greater security to their organizations. For years, the U.S. government has been trying to limit publicly available cryptography and maintain access to the "keys" that permit decoding of the information. Although the public debate over government access is still on-going, it is clear that the U.S. government is losing its grasp on encryption technology.

[25] Tracy Wilkinson, "Safe in Cyberspace, Serbian Protests Flourish on the Net," LA Times, 8 December 1996.

In September of 1996, a committee of wireless communications industry leaders denied the Justice Department access to technology that would allow law enforcement officials to locate and monitor cellular communications within a half-second.[26] E-mail remailers—services that strip or change the origin of an e-mail message,[27]—the use of web sites, and global pagers are other easy ways for an illegal organization to pass messages without fear of capture.

b. Intelligence

The spread of high-tech communications equipment has also allowed network organizations greater ability to collect intelligence. "Such technologies enhance the capabilities of a network's members not only to coordinate with each other, but also to collect intelligence on the external environment and on their opponents...."[28] For example, dozens of commercial imagery satellites—with resolution that rivals that of U.S. military satellites—will be launched in the next three years.[29] Commercial satellite imagery is already available through French and Russian companies, however in addition to selling images from existing databases the new companies will allow customers to aim the satellites at targets of their choosing. This capability allows all types of organizations, including non-state threats, unprecedented capabilities.

[26] John Markoff, "Cellular Industry Rejects U.S. Plan for Surveillance," New York Times, 20 September 1996.

[27] Joshua Quittner, "From god@heaven.org: The Web is 'Anonymous'," Time, 2 September, 1996, 57.

[28] Arquilla and Ronfeldt, 1996, 15.

[29] William J. Broad, "Private Ventures Hope For Profits on Spy Satellites," New York Times, 10 February 1997.

Computers and telecommunications technology also give a greater ability to collect intelligence information. The Internet and other privately maintained databases contain huge amounts of data, personal and otherwise. Years ago accessing sensitive materials via computer required an in-depth knowledge of computer "hacking" and a variety of "hacker tools." Now, computer programs like "SATAN"[30] and information services like Lexus-Nexis give anyone with a limited understanding of computers and a credit card access to a wealth of data. Those "hackers" who do understand the inner workings of computer networks have made even greater strides in accessing information. A team of computer security experts in San Francisco were able to "crack a key part of the electronic code meant to protect the privacy of calls made with the new, digital generation of cellular telephones."[31]

Finally, the Information Age is marked by an explosion in open-source intelligence. With the existence of the Internet and commercial databases, information can no longer be controlled by governments or individuals. The United States has always been an open society, and in order to collect intelligence on the U.S. and adversary simply had to subscribe to Jane's Defense Weekly or attend scientific conferences. The Information Revolution has given even greater access to information than ever before. Open-source

[30] A Unix-based program called the Security Administrator Tool for Analyzing Networks, or SATAN, was designed to automatically probe a network for security holes. In addition to allowing network administrators find holes in their computer networks so they could fix them, it also allowed outside users to find holes in networks and exploit them. SATAN was freely available for download on the Internet.

[31] John Markoff, "Code Set Up to Shield Privacy of Cellular Calls is Breached," New York Times, 20 March 1997.

and commercially available information is becoming increasingly available, challenging the need for expensive government intelligence collection or unwieldy classification systems.

Network organizations are also better able to exploit the intelligence they have. One strength of the networked organization is that all information is available to all members, all the time. Rather than having complex and unwieldy classification systems, the network organizations freely share information with those who require it.

c. Alliances

Because netwar organizations have no firm borders, and the organization is formed along ideological rather than functional lines, alliances are inherent to the network organization. As with the Latin American drug cartels, alliances can, and do, shift constantly based on mutually beneficial arrangements. Weapons traffickers work with guerrilla groups, drug cartels support refugee smugglers, computer hackers are contracted by foreign intelligence services. Strategic alliances based on common goals have become the norm for netwar actors.

Netwar actors may ally with groups on a temporary basis to realize a specific goal, or more lasting alliances may merge new elements into the organization. Some of these alliances may involve state actors, such as the large number of federal officials who have made alliances with the drug cartels in Colombia and Mexico. In the case of terrorist groups, the state may sponsor their organization but not necessarily direct their actions. In the strange world of ethnic warfare, Serbian instructors train Rwandan refugees in Zaire on the art of counterinsurgency warfare, and Ukrainian pilots flying

Yugoslav jets bomb Zairian rebels trying to take control of the country.[32] "TCOs are entering into dark pacts, carving out spheres of influence and making common cause wherever possible..."[33]

These alliances also complicate hierarchical efforts to counter the netwar actors. Hierarchical organizations are organized around a specific function (such as counternarcotics or counterterrorism). However, because of the interconnectedness of the netwar groups, any attempt to fight the threat must then be coordinated with other offices or organizations in order to attack numerous problems simultaneously. This allows netwar organizations to operate in the "gray areas" between organizational responsibilities and take advantage of the weaknesses inherent in bureaucracies.

One area where alliances are readily abundant is in transnational criminal activity. Drug cartels, criminal groups, and arms traffickers are mutually supportive and generate huge profits that allow these groups to operate at a level rivaling some governments. With the breakup of the Soviet regime, Russian military equipment of all kinds are available for rock-bottom prices.[34] In February of 1997, U.S. law enforcement officials soured a deal between Russian arms merchants and Colombian drug traffickers for the purchase of a Russian nuclear submarine.[35] In June of the same year, federal officials, posing as representatives of a Colombian drug cartel, arrested two former Soviet

[32] Howard French, "In Zaire's Eccentric War, Serbs Train Refugee Force," New York Times, 12 February 1997.
[33] Arquilla and Ronfeldt, 1996, 62.
[34] Jonathan Beaty, "Russia's Yard Sale," Time, 18 April 1994, 52-55.
[35] "U.S. Says Drug Smugglers Tried to Buy Sub," Reuters News Service, 7 February 1997.

citizens for attempting to sell Bulgarian-made tactical nuclear weapons and surface-to-air-missiles.[36]

d. Innovation

Of the many strengths of the network structure, it is the netwar actor's use of innovation that is perhaps his greatest asset. Offensively, netwar organizations are adaptable, flexible, and versatile in their response to challenge. "These node-level characteristics, rather than implying the need for rigid command and control of group actions, combine with interoperability to allow for unusual operational flexibility..."[37] Innovation is the ability to recognize and react to change. Because of the decentralized nature of netwar organizations they are able to operate in an innovative manner, exploiting the adversary's weaknesses, learning from their mistakes, and immediately correcting procedures to improve operations.

One example of the high level of innovation that exists in criminal organizations is the widespread use of cloned cellular telephones. In 1992 a career criminal named William Anderson Jr. decided to apply publicly available information on hacking and electronics to criminal enterprise. Linking together a digital scanner, laptop computer, and an antenna, he created a device that would intercept and record ID numbers from cellular phones located in passing cars. Anderson was then able to download the stolen numbers into other cellular phones, reprogramming their memory chips and creating virtual clones of the intercepted phones. Anderson provided these

[36] Catherine Wilson, "Two Accused in Nuke Sale Sting," Associated Press, 30 June 1997.
[37] Arquilla and Ronfeldt, 1996, 11.

phones to his network of drug runners and thieves who would use the phones for a couple days and then return for reprogramming. In addition to making the phones virtually untraceable and untappable, the device also allowed Anderson to listen in on cellular phones used by the local police. Although Anderson was finally captured, the technology he created has proliferated and created an entire new criminal industry: cellular phone cloning. Collection devices have been mailed across the country, collecting numbers the entire way. Cloning plants have sprung up in virtually every major city. Cellular phones have been modified to store up to 99 different numbers that can be changed at the push of a button. In addition to giving criminals free access to cellular communications, law enforcement officials are forced to file separate court orders for each number they wish to tap making it virtually impossible to listen in on criminal's phone conversations.[38]

Aside from being extremely flexible tactically, netwar organizations are able to communicate and institutionalize changes into the organization quickly, enabling organizational innovation. The transfer of the Colombian drug cartels from a hierarchical structure to a networked one was the result of an innovative approach at dealing with guerrilla kidnappings. Where a strictly bureaucratic organization would resist dramatic changes, the drug cartels recognized the implications of combining their resources for more than just security. The tactical innovation of organizing a counter-guerrilla army was not only formally adopted by the cartel organizations, but it led to a structural innovation that revolutionized the way drug cartels organized.

[38] Elaine Shannon, "Reach Out and Waste Someone," Time Digital, July/August 1997, 35-39.

Other organizations are learning from the successes of transnational criminal organizations. Nation-states hostile to the United States witnessed the defeat of Iraq during the Gulf War and are unlikely to attempt attacking the United States with direct military force. Rather, they will likely explore other means of fighting the United States, including the use terrorism and nuclear, chemical, and biological weapons. But these are areas where the United States has policy, experience, and a known response. Countering organizational challenges has proven to be more difficult. If netwar organizations understand the complex nature of Information Warfare, they can exploit the United States' lack of policy and experience, and they can operate inside the confusion surrounding Information Warfare roles, missions, and responses. The lessons of the drug cartel's successful structural transformation are there for anyone to see.

B. RESPONSE

> [The Department of Defense] has evolved into a grouping of large, rigid bureaucracies—services, agencies, boards, and committees—which embrace the past and adapt new technology to fit traditional missions and methods. (1982)
>
> Gen David C. Jones (Ret.)
> Chairman, JCS (1978-82)[39]

With the realization that the U.S. faces an uncertain security environment, it follows that the U.S. security structure must reevaluate its strategy, structure, and processes to determine if they allow for optimal performance. As shown in Chapter II, an

[39] Gen David Jones, "Past Organizational Problems," Joint Forces Quarterly, Autumn 1996, 23. Originally published in series of articles in the New York Times in November 1982.

organization facing environmental uncertainty must actively pursue change or risk decreased performance. When U.S. national security is at stake, there is no room for decreased performance.

Many believe the world is now seeing a "Revolution in Military Affairs" with implications for strategy, doctrine, and organizational structure. This is not unprecedented in history. Blitzkrieg is often used as an example of a *revolution* in warfare (it was the Germans' innovative use of the tank, airplane, and radio in a new way that enabled Blitzkrieg to change the face of war) rather than an *evolution* in warfare (the French and British utilized these three tools separately to support traditional warfighting doctrine). Ideally, the current Revolution in Military Affairs will incorporate technical advances into new doctrine and use new forms of doctrine and organizational structure to optimize performance.

Revolutionary technological change is not new to the U.S. military. For example, the invention of the atomic bomb had a significant impact on the way the world fought future wars. In fact, history shows that military forces often look for the "technological solution" that will give them the decisive edge in battle[40]. There is a saying, "offering the military a technological solution is like offering an alcoholic a glass of wine." It should come as no surprise, then, that the U.S. military has been thinking about the impact of

[40] During World War I, the stalemate created by trench warfare led both the French and the Germans to seek a variety of technological solutions that would give either side a decisive edge. The atomic bomb was a technological solution for quickly ending World War II and preventing a bloody invasion of Japan. Many thought the Unites States would be successful during the Vietnam War due to its superior technology. Even the U.S.-led coalition's success during Desert Storm was credited to advanced technology as much as good soldiering.

advanced computer technology since the mid-1970s when Thomas Rona first coined the term "Information War".[41] However, debate over Information Warfare escalated in the mid-1990s when the services began to call for money to purchase high-tech equipment and a new doctrine for employing advanced technology in revolutionary new ways. The United States is now in the midst of a flurry of activity as each part of the national security structure, and the corporate organizations that support them, try to determine how information technologies will change the nature of war.

The U.S. government is still trying to determine the impact of these technological advances. Admiral William Owens' proposal for a "system of systems" envisioned an interconnected web of intelligence collection systems and artificial intelligence that would show everything within a 200x200x200 square kilometer battlespace. Owens' theory was that everyone would see the same picture of the battlespace, giving commanders the "topsight" they need to make decisions while giving soldiers, sailors, and airmen the "battlespace awareness" required to accomplish their missions. Although Owens retired half-way into his term as Vice Chairman of the Joint Chiefs of Staff, he is still actively involved in attempting to implement changes to the existing national security structure. Others see a much more revolutionary use for technology, including creating an entirely new war-form called "Information Warfare" that would replace, or at least augment, physical destruction with psychological and electronic attack.

[41] In 1976 physicist Thomas Rona presented a paper entitled "Weapons Systems and Information War" at the Boeing Aerospace Company. This is probably the first mention of this new form of warfare.

1. "Information Warfare/Information Operations"

In response to the perceived new threats of the Information Age, the United States is currently planning to conduct Information Warfare (IW), more recently called Information Operations (IO).[42] Information Warfare is a very broad concept that incorporates all aspects of the National Information Infrastructure, including DOD, other government agencies, and corporate America. There is no single, accepted definition of Information Warfare. After four years of debate, the national security structure still hasn't agreed on a definition that is sufficiently broad that it does not limit the scope of operations that would fall under it, yet sufficiently narrow that it provides adequate guidance. For simplicity sake, this study will use the definition used by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I) which is widely accepted in the defense community. Information Warfare is defined as, "actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems while defending one's own information, information-based processes, and information systems."

Apparent in this definition is the offensive and defensive potential of Information Warfare. Offensive IW capabilities are still highly classified, but many of the defensive aspects of U.S. Information Warfare are intended to counter expected offensive capabilities if its adversaries. The Department of Defense experiences hundreds of

[42] For the sake of simplicity, the terms Information Warfare and Information Operations will be used interchangeably. However, this author advocates adopting the broader label of Information Operations as it has implications well outside the limits of warfare.

computer intrusions each year[43] and has even warned of the potential of an "electronic Pearl Harbor."[44] Information Warfare targets can include telecommunications networks, financial systems such as the stock exchange, social security, banking, air traffic control systems and virtually any strategically important corporation.[45] Although offensive Information Warfare would attack such targets, these same targets must be protected in the United States. Protecting the U.S. information infrastructure against attack is proving to be more difficult than anyone imagined, and policy makers are still debating how to best go about it.

Even the public has become increasingly aware of the threat of Information Warfare. In addition to fictional movies such as "Hackers" and "The Net", several well-publicized cyber attacks[46] have increased the public's awareness about the capabilities of computer hackers. Many popular magazines including Time, U.S. News & World Report, Wired and The Economist[47] have run lengthy articles on the threat of Information Warfare.

Yet despite several years worth of papers, conferences, articles, and discussion, there are still great divides between the military services, intelligence agencies, law enforcement organizations, and the corporate world that prevent an integrated U.S.

[43] Pat Cooper, "DOD Takes Offensive on Hackers," Defense News, 18-24 September 1995, 4.
[44] Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," The Washington Post, 16 July 1995.
[45] Ibid., 16.
[46] Clifford Stohl's The Cuckoo's Egg (New York: Simon & Schuster, 1989) chronicles the author's efforts to catch the "Hannover Hacker", a twenty-five year old computer programmer from Germany who broke into several U.S. defense computers for the KGB.
[47] "Onward Cyber Soldiers," Time, 21 August 1995, 38-48. "Warfare 2020," U.S. News & World Report, 5 August 1996, 34-42. "A Farewell to Arms," Wired, May 1997, 51-54, 220-226. "The Future of Warfare," The Economist, 8 March 1997, 15 and 21-24.

response to the challenges of the Information Age. Information Warfare is a much-debated topic, and for every advocate there is also a critic. IW supporters say the United States is already under attack and, because of its reliance on technology, it has much to lose from its inactivity. IW critics see an obsession with technology that would divert money from more traditional, and proven, capabilities. Indeed, there's a danger in relying solely on technology when conducting warfare. For example, a human intelligence asset is much less likely to be tricked by a decoy tank or aircraft than an intelligence analyst looking at satellite imagery. Similarly, it's debatable whether a holographic image of Allah telling Iraqi soldiers to surrender would have any greater effect on the soldiers than a leaflet promising them safe passage and food does.

Along similar lines, one of IW's biggest criticisms is that it assumes conflict in a high-tech environment. How can the United States fight information wars with countries like Haiti or Somalia that have little, if any, reliance on technology? Arguments fly between the "techies" and the "dinosaurs" over the fact that most current adversaries are not high-tech entities, but low-tech groups. By definition, though, Information Warfare does not have to be high-tech. IW includes all operations where the United States attempts to influence a perception or behavior using information, and this information doesn't have to be technology-based.

Other debates rage over the validity of putting soldiers, sailors, and airmen at risk when the United States could instead use cruise missiles or Unmanned Aerial Vehicles to conduct missions. Also, with reduced funding available for military operations, some argue that attacking systems with computers is cheaper than using costly munitions. Others argue that if a system is not physically destroyed it may still be capable of causing damage. These debates are valid, and each side has convincing arguments. What everyone agrees on is enormous growth in information technologies gives the United States opportunities never seen before, and the United States must adapt its doctrine, strategy, and organizational structure to take advantage of them. What cannot be agreed on, however, is how this should be done.

Many Information Warfare advocates speak of the "OODA loop,"[48] and the advantages the United States would gain by investing in high-tech command and control, as well as intelligence, systems that would allow decision makers to outperform their adversaries. Ever since man began conducting war, it's been advantageous to get into the enemy's mind and to interfere with their decision making processes. But although the actual process has not changed, new technology increases the speed with which leaders can complete this decision-making process. Many, including Secretary of Defense William Cohen, argue that the United States must invest in tomorrow's technologies while continuing to plan for today's threats.[49] Investment in high-tech systems may increase the

[48] The OODA loop (Observe, Orient, Decide, Act) was a decision making process introduced by John Boyd, an Air Force fighter pilot, who first applied the concept to air combat. The pilot who continually completed the observe-orient-decide-act process the quickest, he believed, would likely be the victor in an air battle. Recent theorists have applied the OODA loop to all decision making, stating that the leader or military commander who has the tightest OODA loop will be victorious.

[49] The Quadrennial Defense Review identified three options for defense planners to pursue: 1. focus on current threats and opportunities by maintaining the current force structure and foregoing modernization; 2. focus on future threats and opportunities by investing in new systems and reducing current force structures; and 3. aim for a balance of the previous two options by maintaining the force structure and investing in future systems. Leaders of the defense structure chose the middle road, choosing not to commit wholeheartedly to either strategy.

flow of information between different parts of the defense structure, but they cannot overcome the problems involved with choosing the wrong organizational structure. When comparing the decision making cycles, it is just as important to consider the flexibility of the networked structure as the communications equipment employed.

Despite Defense Secretary Cohen's decision to pursue current and future defense strategies, the reality of today is that decreasing military budgets will force decision makers to choose between expensive, high-end systems or cheaper, time-proven equipment. Going back to its definition, Information Warfare involves the actions taken to fight and defend, not the equipment used. It really shouldn't matter what means the United States uses to fight a war, as long as those means allow its leaders to complete the decision making process more quickly than its adversaries. No matter if the adversary is a high-tech hacker or low-tech guerrilla fighter, human beings have the same basic wants, needs, and desires. Without a doubt, technology will play a significant role in the future of warfare, and the United States must take advantage of it. But, it's just as important to understand its adversaries' cultural, ethnic, and religious beliefs of as it is to be able to electronically attack their C2 nodes.

As this thesis argues, choosing the correct organizational structure strongly influences the United States' effectiveness against Information Age adversaries. This is not a concept the U.S. senior leadership has embraced yet. As evidenced by the QDR and other documents that will be reviewed below, planners are not seriously considering the limitations inherent in bureaucratic organizations.

2. Strategic Vision of the Future

In order to determine how different organizations making up the national security structure are planning to redesign themselves for the future, it is useful to examine the "strategic vision" that has been presented to the military services and other organizations to lead them into the Information Age. Guiding all services and agencies is the President's National Security Strategy, a document that reviews the security environment and provides goals for those who protect the nation's security. From that, the Chairman of the Joint Chiefs of Staff designs a National Military Strategy to set goals for the military services. Additionally, in 1996 the Chairman proposed Joint Vision 2010 to guide the services in their efforts to redesign themselves to meet future challenges. Finally, each individual service designs their own strategy to meet the designated threats and reach service goals. Other support agencies, including the national intelligence services and law enforcement agencies, also create a vision statement based on the National Security Strategy.

Although the focus of this thesis is not to compare individual services or organizations in their efforts to reorganize, it is useful to briefly examine the efforts made by individual parts of the national security structure. In 1994, the Army proposed Force XXI, a concept calling for new organizational structure and information-based systems to create an Army that is, "not only versatile and responsive, but one that can adapt effectively to that changing world." The Marine Corps created Operational Maneuver from the Sea and Sea Dragon which also call for new organizational forms in order to operate in the Information Age. The Air Force released Cornerstones of Information Warfare, which presents its view of the new roles and missions Information Warfare has created for its service, but calls for doctrinal as opposed to structural changes. Despite an increased awareness of the need for organizational change by some services, none of the documents released has yet suggested how to go about the reorganization of a firmly entrenched, bureaucratic system.

3. Ad-Hoc, Multi-Agency Participation and Coordination

It is clear that security planners are just in the beginning stages of preparing for conflict in the Information Age. Most service plans call for changes to be made in the next few decades (Joint Vision 2010, Air Force 2025, etc.) Yet most everyone agrees the threat is here and now. As evidenced by the previous section, there are a variety of groups that have benefited from the Information Age and some pose a threat to U.S. national security today. These groups are learning the lessons of the Information Age, and are not likely to wait decades until the U.S. is organizationally prepared to face them in conflict.

This is not to suggest that the U.S. national security structure has become ineffectual in the face of these new threats. The U.S. has always responded to challenges from all points on the spectrum of conflict, often using its superior technology and professional forces to deal with the threat. However, much of what has been successful in countering Information Age threats so far has been ad-hoc and informal in nature. Through individual innovation and informal networking, the "get the job done" attitude of personnel in the military, intelligence, and law enforcement organizations has insured the U.S. has met these new challenges. Yet these "quick fixes" are seldom formalized and institutionalized by the organization. Generally there is the "correct" way to conduct business, and then there is the way things are actually done. But as was shown in Chapter II, unless an organization adapts its strategy, structure, and processes to meet the new environmental challenges the organization isn't working at peak performance. It is largely due to the informal connections that the U.S. has dealt with recent challenges as effectively as it has, but the formal boundaries that the bureaucracy imposes on the national security organizations prevent the security structure from taking advantage of its full potential.

After reviewing the literature and attending numerous conferences on the subject of Information Warfare, this author concludes that the United States is preparing to organize to fight Information Warfare in much the same ways it organized to fight the drug war: hierarchically. The following section describes efforts that are currently being taken by the U.S. national security organizations to conduct operations in the Information Age.

a. Command and Control

While generally recognizing the decentralized nature of future threats, U.S. national security organizations are organizing Information Warfare units and centers using a hierarchical command structure. Despite claims that Information Warfare will break down the stovepipes that channel information vertically, most of the new organizations that are being formed under the guise of Information Warfare are vertically structured. Within the Department of Defense, where Information Warfare represents a new mission in a period of drawdowns, each service has set up their own Information Warfare centers, units, and training courses.

The following is a partial list of the organizations created to deal with Information Warfare. While some of these organizations supposedly only play a support role—for instance, officers at the Air Force Information Warfare Center claim they do not "do" Information Warfare but simply assist commanders who request their help—several of these organizations are intended to actually conduct Information Warfare missions. Also, some of these organizations are not truly new, but are simply organizations that performed information warfare-like duties and were subsequently renamed.

The Air Force established the Air Force Information Warfare Center (AFIWC) in 1993 at Kelly AFB, Texas. The mission of the AFIWC is to "develop, maintain and deploy Information Warfare/Command and Control Warfare (IW/C2W) capabilities in support of operations, campaign planning, acquisition and testing." Organizationally, the AFIWC comes under the Air Intelligence Agency as opposed to a combatant command. However, the 609th Information Warfare Squadron, activated in October 1995, is part of the Air Combat Command and is intended to be an operational unit that conducts Information Warfare.[50] The Air Force also created an Information Warfare Training Lab, opened in 1996, to teach offensive and defensive aspects of

[50] Steven Watkins, "New Era has Humble Start," Air Force Times, 20 November 1995.

Information Warfare.[51] Most of the Air Force's IW efforts focus on computer attacks and system protection.

The Army created the Land Information Warfare Activity (LIWA) in 1994 at Fort Belvoir, Virginia. LIWA's is the Army's operational focal point and executive agent for Information Operations and Command and Control Warfare. It falls under command of the U.S. Army Information Systems Command (USAINSCOM) and is primarily concerned with integrating operational security, military deception, psychological operations, electronic warfare, and physical destruction to support Information Operations and C2W. Due to its land focus, the Marine Corps is also involved with LIWA. The Army's IW focus has been on integrating the five pillars on Command and Control Warfare to support ground operations.

The executive agent for Information Warfare in the Navy is the Director of Space and Electronic Warfare who is responsible for IW/C2W development and guidance. The Navy also created two centers to focus on Information Warfare. The Navy's Information Warfare Activity (NIWA) was opened at Ft. Meade, Maryland in 1994. NIWA works closely with the National Security Agency, Office of Naval Intelligence, and the Naval Research Laboratory to conduct research and develop techniques to support Information Warfare efforts. The Fleet Information Warfare Activity (FIWA), opened in 1995 at Little Creek Amphibious Base in Virginia, is tasked with supporting Information

[51] "USAF Opens First Information Warfare Training Laboratory," Internet: www.infowar.com/mil_c4I/mil_c4io.html-ssi.

Warfare activities.[52] Neither of these two organizations have operational IW missions. Much of the Navy's IW expertise resides in the realm of cryptography and deception.

Various other organizations have Information Warfare related centers. The Defense Information Systems Agency (DISA) has always been in the business of network security and has a Center for Information Systems Security. The Federal Bureau of Investigation recently opened the Computer Intrusion Threat Assessment Center (CITAC) which monitors and investigates computer crimes. The Air Force's Office of Special Investigations (AFOSI) also has a computer crimes division that investigates cases involving computer intrusion.

Similarly, all three national intelligence agencies—the National Security Agency, the Central Intelligence Agency and the Defense Intelligence Agency—have established Information Warfare offices or branches within their organizations. Additionally, the Department of Defense is in the process of setting up a joint center at Ft. Meade, Maryland. The Information Operations Technology Center (IOTC) is scheduled to open in July 1997. Several organizations—including the Air Force, Army, and DISA—have established Computer Emergency Response Teams that can be called on short notice in the event of an intrusion into a computer network.

What is perhaps most significant is that each of the organizations mentioned created these Information Warfare centers and units without any direction from the U.S. senior leadership. The President established an Information Infrastructure Task

[52] Robert Ackerman, "Navy Doctrine, Systems Face Information Warfare Makeover," Signal, July 1996, 57-60.

Force (IITF) in 1993, which focuses on privacy and intellectual property rights issues; and the U.S. Security Policy Board in 1994, intended to discuss and recommend policy directives regarding, among other things, information systems security and risk management. However, both these organizations are advisory in nature, and are made up of such diverse actors[53] that there has been little consensus regarding the issues discussed in this study. Even the President's 1997 National Security Strategy makes no mention of Information Warfare, and only makes passing remarks regarding the vulnerability of the United States' electronic infrastructures. The President's guidance—his strategic vision, so to speak—is for those responsible to implement measures to protect the nation's information infrastructure. Without more specific guidance, it is likely that each part of the national defense structure will create capabilities and missions in its own image.

Perhaps it could be argued that the "innovation from below" seen in each organization's creation of Information Warfare centers and units proves that the national security structure is decentralized. However, an alternate theory is that each sees an opportunity to secure their position in the realm of Information Warfare, and wish to enjoy the new funds associated with it. Without strategic guidance from the President, the

[53] Offices represented in the U.S. Security Policy Board, and the associated Security Policy Forum and Overseas Security Policy Board, include: Office of the Secretary of Defense, Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, Department of Commerce, Department of Treasury, Department of State, Department of Transportation, Office of Personnel Management, Department of Energy, Federal Bureau of Investigation, Department of Justice, Information Security Oversight Office, National Communications System, National Reconnaissance Office, Office of Management and Budget, General Services Administration, Joint Chiefs of Staff, U.S. Army, U.S. Air Force, U.S. Marine Corps, U.S. Navy, U.S. Coast Guard, Federal Emergency Management Agency, Nuclear Regulatory Commission, National Aeronautics and Space Administration, Center for Security Evaluations, Foreign Agricultural Service, U.S. Information Agency, Federal Aviation Administration, Agency for Internal Development, Arms Control Disarmament Agency, and the Peace Corps.

national security structure is simply creating organizations in their own image, and fitting Information Warfare into the existing hierarchies.

b. Intelligence

There is little doubt that intelligence will play an important role in the Information Age. The national intelligence agencies have not been left behind in establishing offices to focus on the IW threat. However, as previously mentioned, these organizations simply created an additional block in their bureaucracies to deal with IW.

The role of intelligence has always been to collect pieces of information and weave them together to create a complete picture of the security environment. Cold War intelligence analysts were able to limit their view of the world to the U.S.-Soviet competition. Today's intelligence community must consider a much wider range of threats, and help come up with new means of measuring the threat to U.S. national security. This change involves more than just shifting geographic focus from Central Europe to other regions of the world. It means changing the way the national security structure predicts, classifies, and responds to threats. Traditionally, intelligence organizations connect points of historical knowledge to predict the future behavior of U.S. adversaries. But there is only a limited knowledge of Information Age threats, and thus it becomes increasingly difficult to predict their future behavior. The intelligence community must actively look for these new threats, and seek to learn their patterns of behavior.

Thus far, there has been little motivation for the intelligence community to expand the focus of its collection and analysis efforts beyond the Tier 1 threats of the world.[54] With the limited number of resources available, the intelligence community is forced to prioritize where it will focus its efforts. Budget cuts in intelligence, combined with greater operations tempo and a greater spectrum of threats will spread intelligence assets even more thinly. Yet it is the responsibility of the intelligence community to identify emerging threats before they attain a capability to harm U.S. vital interests.

In today's uncertain security environment, intelligence is more important than ever before. But the intelligence community will face great challenges both in determining new forms of measurement to determine threat and success. Counting equipment and troops is not an effective form of measurement when determining the risk posed by an mercenary hacker ring. The intelligence community will be called on even more to determine intent and motivation, much more risky than simply determining capability. This requires getting into the mind of the enemy, a very different endeavor than simply analyzing imagery and exploiting equipment. Intelligence in the Information Age requires using a new framework of analysis that must be consciously taught and encouraged.

Countering adversary intelligence capabilities is also very difficult. Information is getting harder and harder to control, but the U.S. response has been to find new ways of controlling information rather than learning to live in an open environment. For example, the U.S. government approved the launching of a constellation of commercial spy satellites that rival any the intelligence services maintain. Recognizing the

[54] The U.S. ranks nations by their threat to the U.S., Tier 0-4. Tier 0 nations are those that the United States is at war with. Tier 1 nations (China, North Korea, Cuba) are considered to possess the greatest potential for hostility against the U.S. or its allies.

opportunities that this presents adversaries, the United States response has been to increase its anti-satellite program so that it can permanently disable these satellites in the event of a war.[55] Along the same lines, the military used to be able to control the media's access to the battlefield effectively through use of press pools and news censorship. But with the advent of satellite communications the government has lost its hold on information. Yet conflict between the Department of Defense and the news organizations is still common as the military tries to control media access to regions of conflict.

One technical innovation that may have a revolutionary impact on intelligence dissemination is the classified equivalent to the World Wide Web: Intelink. Intelink brings to the intelligence community what the Local Area Networks (LAN) brought to the business community and the Internet first brought to the academic community, then the world. Instead of each intelligence organization creating and disseminating intelligence products to a select few offices, Intelink allows organizations to post intelligence products and even raw information. Rather than having to request intelligence information and then wait hours or days for it to arrive, an intelligence analyst can actively search Intelink for the information required. The traditional "push" of intelligence may be replaced by the ability to "pull" all intelligence necessary off of Intelink. Like the Internet, users can also send classified e-mail and join chat groups to collaborate on items of interest.

[55] William Broad, "In Era of Satellites, Army Plots Ways to Destroy Them," New York Times, 4 March 1997.

There are some drawbacks to Intelink however. First, the dispersion of the system that carries Intelink, JDIS (Joint Deployable Information System), has been from the top of the organization down. While the most significant application of Intelink is at the lowest levels of the organization, where intelligence personnel interface with operators, the systems have only proliferated to the manager level so far. Also, like the Internet, the vast amount of information available on Intelink makes finding specific information extremely difficult. With the availability of raw data as well as finished intelligence products, "information overload" is as dangerous a possibility as having a shortage of intelligence. Also, cultural barriers still prevent complete information sharing as agencies withhold information in order to protect their sources. Finally, Intelink is largely limited to the military and intelligence organizations, but does not include law enforcement agencies like DEA and FBI.

c. Alliances

There has been a significant amount of debate over the level of information-sharing that should occur regarding Information Warfare. For years, the term "Information Warfare" was classified top secret, and information about IW was not releasable to U.S. allies. Much of the United States' Information Warfare capabilities still exist as "black" programs well outside the view of the defense community. Even today there are some who believe the public debate surrounding IW is damaging to U.S. security interests because it identifies our capabilities and weaknesses.

However, it is equally clear that the U.S. is not likely to face future threats alone. According to the 1997 National Security Strategy, "No one nation can defeat these threats alone. Accordingly, a central thrust of our strategy is to adapt our security relationships with key nations around the world to combat these threats to common interests." However, this requires the U.S. to share sensitive intelligence information and assets with partners who may only be temporary allies or coalition members. The difficulties of sharing intelligence between U.S. organizations and agencies will be exacerbated when applied to the international arena. One significant lesson of the drug war is that with non-state threats the response must be regional rather than unilateral. The same is true with the threats of the Information Age. The Internet and global communications have broken down the barriers between countries, and alliances are more important than ever. This is especially true when combating non-state threats that often enjoy free movement across international borders which U.S. security organizations are forced to respect.

Admiral William Owens and Joseph Nye, Jr. suggest that the United States should extend an "information umbrella" over its allies much like the nuclear umbrella of the Cold War.[56] The goal would be to encourage global information sharing, and an openness that would reduce the threat of conflict. "If the United States is willing to share this [pre-crisis] transparency, it will be better able to build opposing coalitions before aggression has occurred.... Now the central issue is ambiguity about the type and degree

[56] Admiral William A. Owens and Joseph S. Nye, Jr., "America's Information Edge," Foreign Affairs, March/April 1996, 20-36.

of threats, and the basis for cooperation is the capability to clarify and cut through that ambiguity."[57]

Aside from problems with international alliances, there are even problems regarding alliances of different parts of the national security structure. The U.S. military believes it has taken the lead in preparing to fight Information Warfare. Despite this, each service has its own perspective on what Information Warfare is, and what role their service will play if the United States were to wage an Information War. However, many corporate businesses do not want the government involved in protecting commercial networks or institutions. The Information Age has seen many good relations emerge between government organizations and corporate interests. But others feel government regulation has a negative effect on their business and often remark "the market will take care of itself." Just one example of the conflict between government and corporate interests is the debate over commercial cryptography. Fearing the loss of control over monitoring communications, the government wants "back door" access to all publicly available cryptography as well as forbidding export of cryptography overseas. Computer companies wanting to cash in on secure networks, and corporations with transnational offices that want to protect their overseas communications, are against government intervention.

The question of conducting Information Warfare also brings up a plethora of legal questions that may prevent a unified response to information attacks. For

[57] Ibid., 26.

example, what responsibility does the Defense Department have in helping to protect commercial phone lines that carry as much military communications as civilian communications? Can a military CERT respond to a cyber-attack on a bank that primarily services military members? What happens if the bank, fearing loss of public confidence, doesn't want to disclose that there has even been an attack? Unfortunately this raises more questions than it answers, but clearly the United States faces challenges when presenting a unified response to the new threats of the Information Age.

d. Innovation

Some believe the U.S. national security structure is going through an unprecedented period of innovative thinking. The military services have embraced Edward Deming's leadership philosophy, called "Total Quality Management" (TQM). Despite the top-down leadership approach of the bureaucratic military services, TQM allows individuals at all levels to recommend changes to improve processes and operations. Senior military commanders encourage "out of the box" thinking, a euphemism for creative problem solving.

However there is little evidence to suggest that innovative thinking has become part of the security structure's culture, or that organizational innovation will change the structure of the military, law enforcement, or intelligence organizations. As seen in Chapter II, creating an innovative organization is difficult at best. Bureaucratic organizations like the national security structure, by design, tend to resist change and stifle innovation. The changes required to make the many diverse organizations that form the national security structure truly innovative would be overwhelming. Change would have to be deep, pervasive, and affect large portions of the organization. March and Simon perfectly describe the phenomenon that is occurring in the defense community today: "satisficing." The rise of netwar threats has been subtle and poses only a minor threat to U.S. national security compared to the threat that existed during the Cold War. Similarly, there has been neither a recent military failure, nor intervention from civilian oversight to force the military into innovation.

For these reasons, it is unlikely that innovation will become an integral part of the national security structure without senior leaders becoming aware of its benefits, and the dangers of resisting change. While tactical innovation and informal networks will likely continue to provide "fixes" for organizational problems in the national security community, true organizational innovation is not apparent or likely.

C. RESULT

The new security environment described will require an unprecedented level of internal coordination and cooperation between the three distinct groups that make up the national security structure. It will also require breaking down traditional barriers and involving organizations not previously considered in the past. The old organizational forms, hierarchical organizations, seem to be inadequate to coordinate in the face of more agile, networked threats of the Information Age. Radical organizational changes may be needed to make operations involving the military, law enforcement, and intelligence organizations more seamless. Currently there exists a system in which intelligence agencies hold back vital intelligence to protect their sources, and local law enforcement officials withhold information on drug deals in order to get all the credit (and the seized assets) when they cross through their jurisdiction.

The United States also has a military that is prevented from operating on U.S. soil or assuming law enforcement functions. Similarly, the national intelligence agencies are forbidden from collecting against American citizens anywhere in the world, forcing collection efforts to end when a U.S. citizen is involved. Finally, international laws and operations are severely limited by non-participants and weak governments that pay lip service to supporting international security efforts.

The old concept of deliberate planning, based on a thorough understanding of the threat, is ineffectual with the wide variety of threats that the U.S. now faces. Crisis action planning,[58] where plans are developed in hours or days, has become the norm in military operations of the post-Cold War era. In addition to requiring flexible and mobile forces to respond, this also requires more innovative and comprehensive intelligence analysis to give decision makers as much notice as possible of potential crises. This requires a shift from deliberate planning, which gives the national security structure time to identify, plan for, and respond to an attack, to crisis action planning, which requires that the security structure to be flexible, innovative, and already understand what the U.S. leadership

[58] Joint Pub 5-0, Doctrine for Planning Joint Operations, defines Crisis Action Planning as "the time-sensitive planning for the deployment, employment, and sustainment of assigned and allocated forces and resources that occurs in response to a situation that may result in actual military operations. Crisis action planners base their plan on the circumstances that exist at the time planning occurs."

wants. This would require a significant change in the strategy and structure of the national defense community.

Unfortunately, the system that served to protect U.S. national security for the past 50 years was built to operate in a static environment and resist dramatic change. The unanticipated demise of the Soviet Union as a threat has left a void in the security structure that has yet to be filled by another peer competitor. In the past five years the U.S. military has gone through three major policy reviews—the Bottom-Up Review, the Roles and Missions Commission, and the Quadrennial Defense Review—in order to determine what the force structure should look like in the post-Cold War era. Yet each review determined that the U.S. has the strongest military forces in the world, and drastic change is not necessary.[59] This indicates that decision-makers at the highest levels don't see the need to radically reorganize or increase military or intelligence organizations. Yet it is clear that the U.S. security organizations must change in the face of the new security environment.

Without improved coordination, the low-end threats of the future could simply outperform the security structure currently set up to protect U.S. vital interests. This is especially true if the organizations know the rules (as they most likely do) and intentionally operate in the gray area where U.S. security organizations have the most difficulty coordinating. For example, a Mexican drug cartel may realize that its communications will most likely be intercepted and require every communication to consist of at least one

[59] Other findings conclude that: the military will have to conduct broader missions while still maintaining its capability to fight in two major regional conflicts; information technology is becoming increasingly important; and defense funding will remain limited.

Mexican and one American. This complicates the responsibility of interception—national intelligence services can't collect information on American citizens and the law-enforcement agencies do not have adequate equipment—and could result in lost intelligence that could be used to counter drug shipments.

The 1997 Quadrennial Defense Review (QDR) shows that U.S. leadership has recognized the need to reevaluate some parts of the national security structure in the face of new threats. However, since the QDR report was released the Defense Department has faced criticism that the report was budget driven, and that it did not go far enough in recognizing changes in the national security environment.[60] Although Secretary Cohen calls for reengineering certain military functions based on the "Revolution in Business Affairs," this restructuring largely deals with infrastructure and acquisition, not decentralization of combat forces. The more important issue is how future forces will need to be organized to manage conflict in this radically new form of warfare. The QDR report repeatedly endorses the ideas proposed in Joint Vision 2010, but it is not clear how the bureaucratic organizational structure and unique culture of the military should be changed. There has been little or no effort made to increase coordination between the domestic and international aspects of the national security structure.

Despite all this, even assuming the national security structure does recognize the need for change, it is uncertain how quickly changes could be made and how widely they would be accepted. Based on the theory of innovation discussed previously, radical

[60] "Defense Experts Criticize Pentagon," Associated Press, 13 May 1997.

change of the military usually follows a period of great defeat or from external pressure. However, the United States won both the Cold War and the Gulf War, and the only external guidance to the military and intelligence services since the end of the Cold War has been to demobilize forces and cut infrastructure. Even the Defense Reorganization Act of 1986, which streamlined joint military operations and is now recognized as a vast improvement, was initially forced on an unwilling military by external actors. Because of the dramatic changes involved with the Goldwater-Nichols Act, many senior commanders fought against Congress making any changes to the defense organization.[61]

[61] According to one former Chairman during the organizational review "many have feared that raising basic organizational issues might distract attention from the budget and give ammunition to opponents, who would use admissions of organizational inefficiency to argue for further budget cuts." (Gen David Jones, "Past Organizational Problems," Joint Forces Quarterly, Autumn 1996, 27.) According to current Chairman, Gen John Shalikashvili, "[t]he forces against change were strong. Not only were there open and persuasive advocates of the status quo, but the effects of some changes were hard to predict and entailed considerable risk." ("A Word From the Chairman," Joint Forces Quarterly, Autumn 1996, 5.)

V. IMPLICATIONS FOR ORGANIZING IN THE INFORMATION AGE

May you live in interesting times.

An ancient Chinese curse

It is clear from the preceding chapters that the global security environment has changed dramatically over the last 10 years, and will likely keep on changing. The Information Age has brought about changes in the world that are having a significant impact on how the U.S. national security structure operates. Rather than predicting threats that may come about years in the future, this study showed that there are already a range of new and old threats that are taking advantage of the opportunities presented by Information Age technologies and the post-Cold War environment. One significant advantage, as a result of advances in communications technology, is that organizations can decentralize and disperse themselves while maintaining constant contact. Many groups that pose a threat to U.S. national security have already learned the benefits of adopting a networked structure. However, the Information Age also presents opportunities for the United States. In order to remain competitive in the Information Age, the U.S. national security structure must redesign itself to be flexible and agile. Although no simple task, the security of the United States is at risk. Before reviewing the possible changes, it is useful to go back and see if this study has answered the questions posed in Chapter I.

This thesis attempted to answer two broad questions. The first question was: under what conditions do organizations innovate and reconfigure themselves for optimal performance? From the review of organization theory, one can see that there is no simple answer to this question. There are a great number of factors that go into determining whether an organization will embrace or resist change in response to changes in its environment. Typically, hierarchical organizations resist change and thrive in a complex but stable environment. Organizations that are more decentralized, such as network organizations, tend to embrace change in response to a dynamic operating environment. However, there is no single solution to the challenge of environmental change. Rather than following a checklist for organizational redesign, an organization must conduct an honest assessment of its environment to determine what changes are necessary. At the same time, an organization must become intimately aware of its own strengths, weaknesses, capabilities, and goals. The words of Sun Tzu, who wrote "If you know the enemy and know yourself, you need not fear the result of a hundred battles,"[1] remain true today.

The second question posed was: how has the Information Age changed the organizational requirements for the U.S. national security structure? This question is easier to answer, though no easier to enact. There are basically three organizational paths that the national security structure can follow when preparing for conflict in the Information Age: continue down the hierarchical path, adopt an entirely networked structure, or establish a hybrid structure that combines elements of both the hierarchy and the network. This chapter will review the pro's and con's of each of these three paths.

[1] Sun Tzu, The Art of War, edited by James Clavell, New York: Dell Publishing, 1983, 2.

A. CONTINUED HIERARCHICAL STRUCTURE

This path, maintaining the same organizational structure that has effectively protected the United States for the past 50 years, seems the safest and simplest approach. With this path, the defense organizations would look very much like they do today. The nation would maintain a large and complex security organization to protect against threats to the United States and its allies. The task of protecting the nation would continue to be subdivided, and there would be clear distinctions made between protection from internal and external threats. Numerous parts of the security structure would continue to fill their particular roles in protecting the United States and its allies from any organization that poses a threat. Each part of the defense organization would specialize in specific tasks that relate to their area of responsibility. There would be strict controls placed on each part of the organization, and on individuals within the organization, to ensure that each part performed as required. A large percent of personnel would be utilized as managers and staff officers to make sure that everyone was doing the right thing, in the right order, at the right time.

These four factors—size, role clarity, specialization, and control—represent the attributes that nearly all large organizations shared over the past 50 years.[2] With the hierarchical path, the barriers between different parts of the organization would be strong and there would be very little crossflow between parts. Decision making would come from the top of the organization and would flow down, with very little individual initiative permitted below the highest levels of management. There would be strong distinctions

[2] Ron Ashkenas, Dave Urlich, Todd Jick, and Steve Kerr, The Boundaryless Organization, San Francisco: Jossey-Bass Inc., 1995, 6.

between members of the organization and outsiders, and each part of the organization would maintain its own support functions.

Despite its often bulky appearance, the hierarchical structure is not inherently flawed. There are ways to improve the bureaucracy (improving vertical information systems, creating lateral relations) without discarding the traditional hierarchical structure. But the current national security structure is suffering from an "unhealthy hierarchy."[3] The warning signs are clear. The security structure has a slow response time; takes too long to make decisions and react to environmental changes; displays rigidity toward change by doing things because it is the way they have always been done; and leads to internal frustration with employees and managers feeling dissatisfied with the organization and unrecognized for their work. These are all symptoms that the hierarchy has stagnated. In order to solve some of these problems, the hierarchy's vertical boundaries would have to be loosened somewhat.

1. Pro's

Continued use of the hierarchical structure would entail the least amount of change, and small adjustments could be implemented to make it more responsive to environmental changes. By choosing this path, senior leaders would not be faced with changing the specific cultures of the many organizations that make up the national security structure. They would also be spared the difficult task of amending laws and removing barriers that have separated military, law enforcement, and intelligence functions for decades.

[3] Ibid., 41.

2. Con's

With the rapidly changing environment that exists today, it is not likely that hierarchical organizations could produce the speed, flexibility, and quality of decision making that more decentralized structures would give. In light of the drastic changes in the security environment, it is clear that the horizontal boundaries separating U.S. security organizations are in fact hindering operations. Criminal organizations are operating in the gray-area between organizational boundaries, and it is only a matter of time before rogue nations learn these lessons. Cultural differences of the many organizations act as barriers to integration, despite the need for coordinated operations. Embracing high-tech systems and changing doctrine may not be enough to enable the U.S. security structure to keep up with the nimble netwar threats. Adversaries of the United States are already modifying their structures to take advantage of new forms of organization, and netwar organizations' use of technology and organizational change may quicken their decision making processes, giving them a competitive edge in conflict.

B. CHANGE TO NETWORK STRUCTURE

This path, adopting an entirely new organizational structure based on the network, would entail dramatic changes to the way the national security organization operates. The large, divisional organizations of the past would be replaced by smaller, task-driven units that emphasize speed in all they do. Rather than subdividing tasks and delineating lines of authority, the network organization would encourage flexibility by discarding job descriptions and encouraging multi-disciplinary teams and offices. Rather than having different parts of the organization specialize in particular tasks, the network organization would integrate capabilities to fit a particular situation. Controls and management would be replaced with innovative cultures that reward creativity and goal accomplishment.

These four factors—speed, flexibility, integration, and innovation—are the attributes that organizations are seeking to adopt to take advantage of the opportunities presented in the Information Age.[4] Strict, immovable boundaries between organizations would be replaced by permeable, flexible ones that allow for rapid movement of information, supplies, and personnel. Decision making would be decentralized, encouraging individual initiative at the lowest levels of the organization. External boundaries would be difficult to discern, and many aspects of the organization's processes would be contracted out or supplied through strategic alliances.

In the case of the national security structure, the National Security Council (NSC) has authority over protecting the security of the United States. The NSC would act as the core of the organization (providing strategic guidance for the organization) and acting as the network integrator (bringing together the necessary resources to protect the nation.) This is not significantly different than the system that exists today, but would require greater decentralization to allow individual services and agencies in the national security structure to specialize in specific functions while tasking other parts of the organization when their capabilities are required. It would require greater information exchange and decentralized operations to take advantage of the inherent flexibility of the network.

[4] Ibid., 7.

Accountability could still be maintained using connectivity and communication rather than vertical reporting

1. Pro's

The network structure would take advantage of technological advances to produce agility, flexibility, integration, and innovation in an organization. These four factors are as beneficial in security environments as they are in business environments. U.S. leaders have already accepted that investing in technology is important to remain viable in the post-Cold War world, so perhaps there would be support for investing in new organizational structures as well. The network structure would also give the benefits of a large organization when it is advantageous (purchasing equipment and supplies in large numbers, etc.) while allowing the organization to act like a small unit when it is beneficial (problem solving, quick decision making, etc.) Advocates of IW use the OODA loop to show the value in making decisions more quickly than the adversary. The decentralization of the network structure would not only allow greater speed in decision making, but it also would allow leaders to make midcourse adjustments in order to correct mistakes.[5]

2. Con's

Adopting a network structure might not be possible for an organization that embraces tradition and rules. The bureaucratic culture that exists, especially in the military, of unquestioningly following orders without knowing the "big picture" may be a necessity considering the nature of the task. Similarly, the hierarchical rank structure provides order in a profession that requires order to accomplish its primary task of fighting

[5] Jay Galbraith, Edward Lawler III, "Challenges to the Established Order," in Organizing for the Future, San Francisco: Jossey-Bass Publishers, 1993, 5.

wars. One great strength of the hierarchical military structure is its high degree of role standardization. Pieces can be exchanged with very little disruption in operations. During wartime there has traditionally been a high degree of attrition, and the standardization of troops makes it easy to replace those who have been killed off in battle. The military is a quintessential hierarchy, and its very nature may require that it maintain a largely hierarchical structure.

C. HIERARCHY-NETWORK HYBRID

This path, integrating certain aspects of the network structure into the existing bureaucracy, would create an organization that utilizes different structures for different functions. Although traditional organizational units would remain intact, lateral relations would allow the creation of multi-agency teams that resemble small units. These teams—often called "task forces" in the national security community—would either be temporary or permanent and would be given a specific task but not told how to accomplish it. While maintaining different levels of authority, tasks and responsibilities would be shared by all members with a stake in the organization. Roles that are core to the organization would be specialized, while supporting functions would be subcontracted from other organizations. Standardized procedures and controls would be retained for the static parts of the organization (finance, administration, etc.) while units that encounter a high level of operational uncertainty would be given flexibility in accomplishing assigned tasks.

This setup is similar to that of many successful business corporations that are experimenting with loosening their bureaucratic structures, but are not willing (or able) to reorganize into a fully networked structure. Boundaries between organizations would distinguishable, but permeable. Decision making would be centralized but interactive, and innovation would be encouraged to perform non-standard tasks. External boundaries would give workers a sense of belonging to an organization, but would not interfere with inter-organizational coordination.

With this path, the hierarchy would still provide the framework for the national security structure, but lateral relations would become formalized, and cross-organizational communication and coordination would be the norm. Strategic alliances would form between different parts of the organization to combat specific problems, and information would pass unimpeded between organizational components.

1. Pro's

The hybrid form of organizational design would retain many of the positive aspects of the hierarchical structure, yet would allow some of the flexibility and agility of the networked organization. Because the basic structure of the organization would not be dramatically changed, there would be less resistance from those who fear change. Many parts of the organization that continue to operate in a static environment, such as finance and many support functions, may not need changing. The hybrid structure allows only the organizations that would benefit from change to adopt new structures.

Information Warfare supporters already envision the "system of systems" that would coordinate information from all parts of the national security structure, and information-sharing would become an integral part of the hybrid structure. The national security structure already allows some degree of lateral coordination in the form of personnel exchanges (liaisons from one organization permanently assigned to another organization for purposes of coordination) and co-location of personnel (housing various organizations in the same building or geographic area, to allow for informal networking and coordination.) In fact, the complex network of personal contacts that a security professional establishes throughout his career is an informal means of lateral coordination. The hybrid organization would simply encourage and assist in forming these personal contacts.

2. Con's

Despite its improved structure, the hybrid organization would retain some of the limiting traits of a bureaucracy, while reducing the speed and flexibility inherent in the network. Authority relationships and organizational boundaries would exist, but leaders would be asked to give up some of their authority and control. Also, creating a hybrid organization would entail redesigning some parts of the organization as networks while leaving others with hierarchical structures. This could create internal barriers (resentment, cultural differences, etc.) between hierarchical and networked parts of the organization. Leaders could also face great problems determining which elements of the organization would be optimized with the network structure and which could remain hierarchical. In many ways, it could be easier to modify the entire organization than it would to change only selected parts.

D. RECOMMENDATIONS

Taking into consideration the danger of maintaining a strictly hierarchical structure in today's uncertain world, and the great difficulty involved in shifting to a completely networked one, the hybrid path seems the most appropriate course of action. While it is easier (and possibly even beneficial) for the national security structure to maintain a hierarchical framework, it is necessary to formalize lateral relations and increase the flow of information between all parts of the national security structure. Rather than relying on command and control to conduct operations, leaders in the national security structure will have to rely on collaboration and coordination between all parts.

Not only does the hybrid structure seem to be the most attainable structural change possible, at least in the near term, it appears to be the most appropriate as well. Some parts of the national security structure have not faced changes to its operating environment. Many functions like pay and finance continue to operate in a static environment, with little change and a highly repetitive function. While this does not mean that such organizations would not benefit from improving its processes, structural change may not be the most appropriate means to improve operations. Each part of the national security organization must evaluate its environment and determine if it would benefit from a looser organizational structure.

In some ways, the U.S. security structure is already headed toward this path, such as its emphasis on joint operations and the acceptance of Total Quality Management principles. However, this course also entails some dramatic changes to the way security organizations operate and relate with each other. Change must be initiated, monitored, and enforced in order for it to be successful, it will not simply happen on its own. The institutionalized borders between organizations must be broken down. Those that resist change must be educated or removed from the organization, as they pose barriers to effective redesign.

The difficulty in shifting to a looser, hybrid structure is that it does not simply involve empowering workers and changing job titles around. It involves a fundamental shift in the way the security structure operates and organizes itself. The hierarchical organization that has predominated for most of the security structure's existence was designed to resist change, and has a tendency to stifle innovation and learning. For organizations to become agile and flexible, they must be able to redesign themselves continually, and undergo large-scale organizational change.[6] The shift to a hybrid structure will not be easy, but it is necessary. Two organization theorists put it best when they wrote, "Our belief, based on our research to date, is that, simply to survive, organizations in the future will have to be able to innovate, to improve their processes, and to redesign themselves."[7] The following are just some of the changes that must be made to the existing security structure.

1. Create an Innovative Culture

Successful organizational change starts with an organization's leadership. The shift to a hybrid structure can only be successful if leaders of the U.S. national security structure (starting with the National Security Council—made up of the President, Vice

[6] Susan Mohrman, and Allan Mohrman, Jr., "Organizational Change and Learning," in Organizing for the Future, 1993, 88.
[7] Ibid., 88.

President, Secretary of Defense, Secretary of State, Director of Central Intelligence, and Chairman of the Joint Chiefs of Staff) embrace the transformation and direct a change in the organization's culture. Senior leaders must be willing to give up some of the controls they once maintained, and they must encourage an innovative and integrative culture in which boundaries between ranks and organizations are less important.

At the same time, they must give all members of the national security structure a common vision of how to respond to the variety of challenges the United States will face in the future. Senior leaders and middle-managers must shift from providing day-to-day decision making to providing long-term guidance and strategic vision. They must constantly be searching the horizon for new trends that can pose an opportunity or threat, and then prepare the lower-levels of the organization to deal with these changes. This requires senior leaders and decision makers to take the "long-view" approach. Rather than being limited by what they know, senior leaders must be constantly thinking about what could happen in the coming months or years.[8] This means embracing a new paradigm of keeping an open mind, seeking inputs from a variety of sources, and making educated guesses about the future. Leaders could take advantage of increased connectivity, using the Internet or an Intranet, to communicate their views and rapidly spread information throughout the entire security structure.

By creating a culture of open-mindedness and flexibility, the entire security structure will become more dynamic and malleable. Change will become an integral part

[8] Peter Schwartz, in his book The Art of the Long View: Planning for the Future in an Uncertain World (New York: Doubleday, 1996), describes his success with scenario-building. He advocates looking at a broad spectrum of alternate futures, and not discounting ideas simply because they seem unrealistic.

of the organization's operating strategy, and innovation will become increasingly more likely due to the open nature of the organization. But simply allowing innovation and individual learning to take place does not ensure that the organization will place value in the new ideas generated. Therefore, new ideas must be integrated into organizational practices, policies, or design features.[9]

Fortunately, the groundwork for this cultural change may already exist. A generation of soldiers, sailors, and airmen are being raised hearing the words "quality," "empowerment," and "continuous improvement." The military's acceptance of Deming's Total Quality Management principles is creating a culture that values innovation, change, and critical thinking. However, this change is coming about slowly and there are still many leaders who resist loosening their controls. Those leaders damage the belief that change can be successful in a bureaucracy, and may make junior workers cynical about the organization's intent. Every effort must be made to spread quality principles throughout the national security structure, and to educate individuals on the benefits of creating an innovative culture. Those that resist these changes have no place in the organization.

The services have also begun to accept the idea of creating centers for innovation, some of which deal specifically with Information Warfare, that are separate from day-to-day operations and are free to test new ideas in a safe environment. This must not only be encouraged, but it must be proliferated throughout the national security structure. These centers provide a central location where innovative ideas can be sent and tested using a variety of means. They can also protect innovators who would normally be ignored, or

[9] Mohrman, and Mohrman, 1993, 89.

even punished, by the bureaucratic system. But there must be a mechanism that translates successful innovations into the operational structure. The innovation centers should become valued parts of the structure, and decision makers should put a high priority on recommendations made by the centers. There should be a high degree of coordination and communication between these centers. For example, the wide spectrum of Information Warfare centers and units should be linked, constantly sharing findings and ideas. These centers should also link with the academic and business communities that are also conducting research on the impact of Information Warfare. One way to do this would be to create a central clearinghouse, a Joint Interagency Information Warfare Center, that would act as a focal point for all IW-related research.

Finally, at very high levels of the U.S. government, there appears to be increasing sensitivity to alternate approaches. For instance, it is promising that Army General Henry Shelton has been nominated as the next Chairman of the Joint Chiefs of Staff. As the former Commander of the U.S. Special Operations Command, Gen Shelton certainly understands the changing nature of the global security environment.

In a recent article, Gen Shelton wrote:

> We cannot predict our future with absolute certainty, but we can make assumptions about the future security environment based on important, observable global political, military, economic, technological and demographic trends. From these trends, we can speculate chaos, not calm, will permeate the geopolitical landscape for the next several years. Although the Cold War is over, we have to face the reality the United States still has enemies—some apparent, others not as obvious.[10]

[10] Gen Henry Shelton, "Special Operations Forces: Looking Ahead," Defense '97, Issue 3, 32.

Special Operations forces have historically been utilized to perform the "non-traditional" missions that other parts of the national security environment have found too difficult using routine strategies and capabilities. The joint Special Operations community is well integrated, and in many ways the it has already adopted many aspects of the networked structure. As Gen Shelton notes, "It's their uniqueness, adaptability, flexibility and reliability that have made them a force of choice today…" Gen Shelton should bring some very useful insights to the policy making arena, and hopefully he can help lead the change in culture that is required to adopt a hybrid structure.

2. Loosen Organizational Boundaries

Aside from creating a culture that encourages innovation and change, leaders of the national security structure must loosen the organizational boundaries (both vertical and horizontal) that separate each part of the structure and make inter-organizational communication difficult. As previously mentioned, advances in information technology are allowing greater connectivity throughout an organization. However, embracing technology is not adequate to realize the new opportunities possible. While communications technology removes some of the organizational barriers by providing connectivity between people, the organization's design determines whether inter-group communication and coordination will take place.[11] Part of the problem is the cultural barriers between different parts of the organization. But cultures can change, as we have seen in the section above. A greater challenge will be for senior leaders to change the laws that currently prohibit the cross-flow of manpower and equipment. The Posse

[11] Jay Galbraith, "The Business Unit of the Future", in Organizing for the Future, 1993, 49.

Comitatus Act that prevents military forces from conducting law enforcement activities limits their participation in countering transnational criminal activity. The law that prohibits intelligence organizations from collecting information on U.S. citizens also presents significant barriers between organizations. These laws must be reviewed and modified, under the guidelines of the U.S. Constitution and the legislative branch, to allow for greater combined operations and a seamless continuum of monitoring, tracking, and capturing transnational threats.

Loosening organizational boundaries means changing the organizational structure of the national security organizations. Prior to the Defense Reorganization Act of 1986 (otherwise know as the Goldwater-Nichols Act) the defense structure was organized as a "Bureaucracy with a Senior 'Management' Team" (Figure 2.3). Each service was an independent organization, and coordination took place largely between the senior leadership and the President. After 1986, with its emphasis on joint planning, operations and task forces, the defense structure moved closer to a "Bureaucracy with Project Teams and Task Forces" (Figure 2.4). However, the Goldwater-Nichols Act only applied to the military and, to some extent, intelligence services. Now, it is time to shift the security structure even farther down the continuum and move towards a "Matrix" (Figure 2.5), or even "Project" (Figure 2.6), organization. Lateral integration must include all aspects of the national security structure, not just the military, intelligence, and law enforcement aspects discussed here. Many other government, non-government, and corporate entities are involved in protecting the United States, and each has become increasingly dependent on the others to operate in today's world. This requires a significant loosening of vertical centralization and of horizontal boundaries, boundaries that have traditionally kept these very diverse organizations separate.

One promising means of lateral integration is the use of task forces and other joint interagency teams. Rather than simply using temporary task forces, like those formed in response to a crisis or single operation, the U.S. security structure must create permanent teams that can tackle some of the most challenging problems. Despite some weaknesses, the Joint Interagency Task Force (JIATF), established to combat drug trafficking, is a good example of an inter-agency organization formed around a common goal. The JIATF brings together members of the military, Coast Guard, and federal law enforcement agencies with a variety of expertise and experience. Members of the JIATF are co-located, and the organization uses a variety of command and control systems to coordinate activities throughout its area of operations.[12] The JIATF could be a working model of what lateral organizations should look like in the future.

Task forces, or joint interagency centers, appear to be the most effective way to provide lateral integration in order to counter specific threats like narcotics and terrorism. Not only do these interagency organizations provide a wide spectrum of expertise, but they create a common culture and unity of purpose that break down traditional barriers to cooperation. The proliferation of task forces should be encouraged wherever multiple agencies and organizations are involved in the same task or are working towards the same goals. However, the joint interagency organizations that exist today still suffer from the problems of accountability (each member is accountable to his parent organization) and

[12] From a presentation posted on the Internet (www.bmh.com/bmh/presentations.html) entitled "Application of Computer Generated Force Technology to Interagency Drug Interdiction."

motivation (systems of rewards and punishments.) Senior leaders must place value in serving on joint staffs, interagency organizations, or attending interservice schools. Rather than simply being a "square filler," joint assignments should be considered an essential part of professional education and career development. While building a service culture is important early in a servicemember's career, it is equally important that he understand the broader security structure and how different parts contribute unique skills and capabilities.

Another team concept which could be emulated at an organizational level is one used by Special Operations forces—especially the Navy SEALs. The SEALs maintain a database of each member's particular experience and skills. When tasked with a mission, SEAL planners create a team based on the particular needs of the mission. For example, one rescue operation in April 1996 called for the evacuation of a civilian sailor who received a leg wound that became severely infected. The sailor's remote location required a SEAL team air drop to his location, medically treat the sailor, and then sail his boat 200 miles to the nearest island with adequate medical and evacuation facilities. The uniqueness of the operation called for members who were free-fall qualified, had medical expertise, and had knowledge of open ocean sailing in his particular type craft. Team members were individually selected based on their expertise, creating the smallest team with all these capabilities.[13] This concept of tracking individual experience (aided by computer technology) and then selecting mission personnel based on their experience (aided by telecommunications technology) could be used to create highly specialized, joint and interagency teams at a moment's notice. Such factors as languages spoken, regional

[13] LCDR Jeff Anderson, "Navy SEALs Use Skills in Dramatic Rescue at Sea," Full Mission Profile, Witner 1996, 11.

experience, and specialized qualifications could be centrally maintained and globally accessible by all parts of the national security structure.

Another barrier to effective lateral coordination, especially between intelligence and operations, is the classification system that exists. Certainly means should be taken to protect sensitive sources and methods of collection. However, commercial imagery and electronic news services should drive a shift away from holding classified information. Radically transforming the existing classification system could encourage better, and more timely, intelligence support and international coordination.

The decentralization necessary to create a hybrid organization will require senior leadership to push decision making authority to the lowest levels of the organization. The role of senior leadership will be to provide strategic direction and goals to lower levels of the organization, while lateral organizations will take on decision making and coordination relating to day-to-day operations.[14] This design resembles the structure currently used by Silicon Graphics, a producer of computer systems. Silicon Graphics maintains a CEO and senior management staff. But instead of getting involved in the daily operations of the company, their role is to articulate the company's vision to all organization members and ensure that information is available at the important nodes where decisions are made. Their philosophy is that with a clearly stated vision, and the availability of information over the company's Intranet (an internal computer network), every member of the organization can independently make decisions using a common context.[15]

[14] Galbraith, 1993, 52.

[15] Lecture by Silicon Graphics CEO Edward McCracken to the Naval Postgraduate School student body on 27 August 1996.

One benefit of loosening hierarchical controls is that staff organizations, created to maintain control over large numbers of forces, can be reduced and reallocated into operational parts of the organization. This is particularly important in light of the post-Cold War drawdown in military and intelligence departments. There is, in fact, a danger to maintaining large staffs. Staff groups were originally designed to prevent the organization from making mistakes. However, the fast-changing nature of conflict in the Information Age means that overanalysis and slow decision making can be more dangerous than doing something incorrectly.[16] This does not mean that staffs will completely disappear from the national security structure. However, their nature must change to fit the organization's new structure. Their role will change from providing rules, regulations and restrictions, to that of providing information and advice that assists, rather than dictates, decision making.[17]

Loosening organizational boundaries does not mean creating a separate Information Warfare organization or career specialty. Many IW theorists believe that computer specialists, intelligence analysts, and selected other career fields should be grouped together in some sort of specialized Information Warfare organization. Martin Libicki and James Halzett (Commander, USN), in their article "Do We Need An Information Corps?",[18] advocate creating a separate service (an Information Corps) in order to standardize systems and create a common culture. However, creating an

[16] Edward Lawler III, and Jay Galbraith, "New Roles for the Staff: Strategic Support and Services," in Organizing for the Future, 1993, 67.
[17] Ibid., 70.
[18] Martin Libicki and James Halzett, "Do We Need an Information Corps?" Joint Forces Quarterly, Autumn 1993.

additional vertical organization to handle Information Warfare simply serves to build additional walls between those who conduct Information Warfare and those who do not. It should be emphasized that every career field is being affected, in some way, by the Information Age. With the broad applications of technology, and the variety of disciplines Information Warfare entails, every member of the national security structure is an "Information Warrior."

3. Create Strategic Alliances

Along with loosening organizational boundaries to permit decentralized decision making and lateral relations, the U.S. security structure must seek to form strategic alliances with a variety of organizations including some not normally associated with national defense.

The previous section already discussed the need for greater lateral integration of the different parts of the national security structure. However, these alliances must extend beyond the traditional boundaries of the U.S. national security structure. Alliances must extend to corporations, non-government organizations, media, academia, and any number of other organizations that can contribute expertise in the protection of the United States. It is clear that U.S. business corporations, especially those in the telecommunications field, are forming closer ties with the national security structure. But other corporations including financial institutions, computer firms, global shipping companies, and even airlines have already joined with the U.S. government to discuss future opportunities and challenges.[19] Even more must be done to involve industry in shaping the new national

[19] Corporations that are involved with talks about protecting the National Information Infrastructure include: AT&T, COMPAQ, Citibank, Intel, Northwest Airlines, and Silicon Graphics.

security structure that embraces alliances rather than creating adversarial relationships that sometimes exist. Similarly, academia offers a rich source of ideas and expertise that can lead to innovative ways of protecting national security. Currently there exists a divide between professors and security professionals, mostly because of the great cultural differences between the two groups. However, there is much to be gained by tapping into the academic brain trust, as one can see from the creation of the Internet which was a combined effort of the U.S. government and the academic world. Finally, the U.S. national security structure is being forced to work with, and in many cases support, non-governmental organizations of all kinds. Many of the areas U.S. military forces are sent also require the assistance of humanitarian relief or international medical support organizations. Military forces are unable to handle all the problems associated with civil unrest or a breakdown in government. Similarly, the non-government organizations often require logistical support and protection from security forces in the region. These are natural alliances that must be embraced.

The boundaryless nature of the threat also means that international alliances must be formed and maintained along these same organizational lines. Rather than condemning weak states for their lack of enforceable laws or effective punishment, the United States should seek to use its position in the world to strengthen these governments and establish even closer relations. Unilateral operations and single-state conflict are things of the past. The globalization of the threat has added an international aspect to conflict, and regional or global responses have become necessary. This requires a unity of effort that crosses traditional geographic boundaries (like that of the transnational criminal organizations), and the U.S. national security structure must work closely with its counterparts in other countries using realistic measures of complicity and effectiveness.

Finally, strategic alliances may even need to be established between the United States and its adversaries. Who better to bring down an international hacker ring than a hacker recruited to infiltrate and collect information for the United States? Much like the Colombian drug cartels that employ Colombian guerrilla groups to protect their crops while at the same time supporting paramilitary groups fighting against the guerrillas, the United States may find some unique capabilities in those groups it seeks to destroy.

An added bonus to combining organizations through strategic alliances is that some believe this leads to an increase in innovation. "Innovations frequently emerge from the blending of multiple perspectives, such as...the combination of two different disciplines. Consequently, innovation is fostered in organizations that promote integration of multiple perspectives by linking the various organizational parts more closely..."[20]

4. Recognize Environmental Uncertainty

Finally, it is of vital importance that all those involved in protecting the United States recognize that the organizational changes recommended here are not a one-time change that ends when the last recommendation is implemented. Unlike the Goldwater-Nichols Act which only requires an organizational review every four years, the next Defense Reorganization Act will require continual evaluation and change. The Information Age is characterized by sweeping and rapid change, and environmental uncertainty will require the security structure to continually evaluate its effectiveness.

[20] Mohrman, and Mohrman, 1993, 93.

Organizational learning and redesign must become a reflex to environmental change and uncertainty.

Also, senior leaders must acknowledge that the deliberate planning process does not allow the flexibility necessary to counter the unpredictable threats of the Information Age. The national security structure has been designed to shape itself to counter known threats in a static environment. But the dynamic global security environment has forced the security structure, notably military and intelligence forces, to scramble at the last minute to deal with constant crises that pop-up almost undetected. The crisis action planning process that is used to respond to these events takes a heavy toll on those who have to make sense of the situation and establish timely response. Changing the security culture to encourage more risk taking when predicting future threats (the job of intelligence) and allowing creative solutions that use all means available (the job of operations) will help reduce the strain currently being felt by security forces today.

Yet despite all the challenges posed by this thesis, perhaps the greatest challenge will be convincing those responsible for implementing change that there is, in fact, a need for organizational redesign. Despite all evidence that there is some sort of change in warfare occurring (whether it be a revolution or evolution), there are still those who do not see a need to change the security structure that exists today. Many believe that technology has only changed capabilities, but not the nature of warfare or the motivation of the United States' adversaries. Some see the end of the Cold War as the end of great conflict and the beginning of an era of peace that requires a much-diminished, but structurally similar, military. Still others believe that the world is witnessing a period of calm that will end when the United States again faces a great superpower. Before any changes can be made to the national security structure, the U.S. senior leadership must be convinced that the conditions exist to warrant widespread, and possibly traumatic, change. It is much more simple to "satisfice" than to take on large-scale organizational change. Once decision makers accept that the level of environmental uncertainty has led to a decrease in the security organization's effectiveness, the entire thrust of the security structure can be put into determining the changes that need to be made.

However, it must be noted that there is a difference between "fixing" a problem and "solving" a problem. Purchasing high-tech systems to increase connectivity and produce topsight are only temporary "fixes" for the long-term threat posed by networked adversaries. Investing in new technologies <u>combined</u> with structural changes will most likely solve the problems that we are already beginning to see in the dawn of the Information Age.

VI. CONCLUSION

The high level of disagreement regarding the nature of conflict in the Information Age demonstrates the problems inherent in a complex bureaucracy that is faced with environmental uncertainty. After several years of debate, and uncountable hours of conferences and meetings, the United States is no closer to having a national strategy for facing the challenges of the post-Cold War era. Yet the spectrum of threats in today's world has widened significantly. In addition to traditional threats from rogue nations and hostile militaries, the United States now faces an increased threat from transnational criminal organizations, cyber-spies, terrorists, and arms proliferators. Without national-level guidance, it is unrealistic to think that the national security structure will suddenly work out its differences and agree to work together in the event of a dreaded "electronic Pearl Harbor."

Change is nothing new for those who protect the nation's security. The national security structure has always been forced to deal with change. The advent of the railroad, steam engine, automobile, machine gun, airplane, and atomic bomb all led to changes in the way wars were fought. But change has been accelerated in the Information Age, with advances in computing and communications technologies affecting more than just warfighting doctrine. Through its review of the structural aspects of organization theory, this thesis makes it clear that the United States cannot ignore the environmental changes brought about by the end of the Cold War and the rise of the Information Age.

The review of innovation theory, both corporate and military, showed that managing organizational change is difficult at best, and can even be risky. Creating an innovative organization is a leadership challenge that involves more than just changing an organization's structure. It involves the creation of new cultures, measures of effectiveness, and even different sorts of organizations. However, ignoring the changing environment will lead to problems that can threaten the security of the United States. Granted these new threats seem less dangerous than that which the United States faced during the Cold War (global nuclear war), however their less-threatening appearance makes current threats even more dangerous, as they are easier to ignore. Similarly, the traditional boundaries that separate military and law enforcement functions, foreign and internal distinctions, and geographic boundaries have all become blurred. As a result, the security organizations that maintain strict organizational boundaries are finding themselves out-maneuvered by their competition, and conflictive with their adversaries.

This thesis also showed that such problems have already been encountered by the United States in its fight against illegal drugs. The case study on the drug war, comparing cartel structures and operations to the U.S. counternarcotics structure, showed that the drug cartels have intentionally adopted a networked structure in order to counter efforts to destroy their organization. The end result of the structural mismatch has been that the drug cartels outperform counternarcotics efforts in virtually every way. Then, by reviewing Arquilla and Ronfeldt's theory of netwar, this thesis showed that other organizations are learning the value of adopting the network structure. Furthermore, the threats the United States will encounter (and is now encountering) will likely be more malicious and damaging than the drug cartels have been. Where the drug cartels are simply looking for profit, other groups are bent on the destruction of the United States government and society.

Fortunately, the national security structure can learn to adapt to this changing environment. Organization theory provides a great number of lessons that corporate organizations have learned from first-hand experience. Organization theorists have shown that it is possible, and in fact desirable, to shift organizational structures to adapt to dynamic environments. Due to the depth and pervasiveness of change required, it is unlikely that the security structure will become networked, no matter how beneficial that may be. But many corporations have found that they can experience many of the benefits of a network (flexibility, speed, innovation) by using a hybrid structure that combines networks and hierarchies in the same organization. The U.S. national security organizations must be willing to make similar changes to their structures, and this is the challenge that faces today's senior leadership.

The findings of this thesis generally support the hypotheses advanced in Chapter I. Looking at current events, it is clear that today's security environment is characterized by a blending of the traditional boundaries between war and peace, and military and law enforcement organizations. While the defense structure is attempting to deal with the problems of drug trafficking, weapons proliferation and computer attacks, it is not optimally structured to counter such agile organizations. The hypotheses regarding organizational design, and the benefits of the network structure, were also shown to be correct. Looking at the Drug War, one can have little doubt that the cartels' organizational structures give then an edge in their conflict with counternarcotics organizations. Netwar threats may not overthrow the U.S. government, or even governments of lesser-developed nations. But they will continue to erode a government's ability to enforce laws and create order. Using as a measure of effectiveness an organization's ability to meet its goals (profits for drug cartels, successful attacks for terrorists), the networked organizations have an advantage over U.S. organizations that mainly react in order to minimize damage rather than taking a proactive role. As other organizations make the shift towards the network structure, it will become even more clear that the network structure gives U.S. adversaries an edge over the hierarchically organized security structure.

This thesis concludes by offering some recommendations as to how the United States can create an innovative and flexible national security structure. These recommendations, however, are inadequate and incomplete. Those with a greater knowledge of organization theory can certainly point to even more significant and revolutionary changes that are necessary. Similarly, this thesis was limited to looking at the structural problems facing national security organizations. Further study is warranted on human resources aspects of competing organizations, comparing the training, motivation, and reward systems of the national security structure versus those of emerging netwar threats.

The purpose of this thesis was simply to highlight the importance of recognizing the new global security environment that the United States operates in today, and suggest that structural change must begin immediately rather than waiting for a sure sign that the world has changed. It is absurd to think that the very same forces that are compelling dramatic changes in corporate structures will not affect the national security structure in similar ways. The lessons of successful organizational redesign are there for all to learn. Like the liberated prisoners who escaped from Plato's cave, many people in the national security community realize that the shadows on the wall represent a greater world that lurks outside. But if U.S. leadership chooses to ignore the reality of today's world, we are all destined to remain prisoner to those who take advantage of its opportunities, whether they wish us well or ill.

BIBLIOGRAPHY

Ackerman, Robert. "Navy Doctrine, Systems Face Information Warfare Makeover." Signal, July 1996, 57-60.

________. "Marine Corps Information Warfare Combines Services' Needs, Defines Their Differences." Signal, July, 1996, 61-62.

"Application of Computer Generated Force Technology to Interagency Drug Interdiction." Internet: www.bmh.com/bmh/presentations.html.

Anderson, Jeff. "Navy SEALs Use Skills in Dramatic Rescue at Sea," Full Mission Profile. Winter 1996, 11-15.

Arquilla, John, and David Ronfeldt. "Cyberwar is coming!" Comparative Strategy, Volume 12, no. 2, 1993, 141-165.

________. The Advent of Netwar. Santa Monica, CA: RAND, 1996.

Ashkenas, Ron, Dave Urlich, Todd Jick, and Steve Kerr. The Boundaryless Organization. San Francisco: Jossey-Bass Inc., 1995.

"Clinton Says Secret Memo Finds War on Drugs Organization Lacking." Associated Press, 4 October 1996.

"Mexico Drug Czar Ousted." Associated Press, 18 February 1997.

"Mexico General Faces Bribe Case." Associated Press, 18 March 1997.

"Defense Experts Criticize Pentagon," Associated Press, 13 May 1997.

Baum, Dan. Smoke and Mirrors. New York: Little, Brown and Co., 1996.

Beaty, Jonathan. "Russia's Yard Sale." Time, 18 Apr 1994, 52-55.

Bolman, Lee, and Terrence Deal. Reframing Organizations. San Francisco: Jossey-Bass Publishers, 1991.

Braunberg, Andrew C. "Air Force Pursues Two-Sided Information Warfare Strategy." Signal, July, 1996, 63-65.

Brewin, Bob, and Elizabeth Sikorovsky. "Hackers Storm DOD Nets." Federal Computer Week, 11 July 1994, 4.

Broad, William. "Private Ventures Hope For Profits on Spy Satellites." New York Times, 10 February 1997.

________. "In Era of Satellites, Army Plots Ways to Destroy Them." New York Times, 4 March 1997.

Campen, Alan, Douglas Dearth, and R. Thomas Goodden, eds. Cyberwar: Securtity, Strategy, and Conflict in the Information Age. Fairfax, VA: AFCEA International Press, 1996.

Cannon, Angie. "$16 Billion Drug Plan Emphasizes Ads, Courts." Miami Herald, 26 February 1997.

Carlin, John. "A Farewell to Arms." Wired, May 1997, 51-54, 220-226.

Chesborough, Henry, and David Teece. "When is Virtual Virtuous? Organizing for Innovation." Harvard Business Review, Jan-Feb, 1996, 65-73.

Cleaver, Harry. "The Zapatistas and the Electronic Fabric of Struggle." 1995, Internet: www.eco.utexas.edu/homepages/faculty/Cleaver/zaps.html

Cooper, Pat. "DOD Takes Offensive on Hackers." Defense News, 18-24 September 1995, 4.

Cyert, Richard, and James March. A Behavioral Theory of the Firm. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1963.

Darling, Juanita. "Short Prison Terms of Freed Drug Lords Rile Colombians." Los Angeles Times, 21 September 1996.

DiNardo, R. L., and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." Airpower Journal, Vol. 9, no. 4, Winter 1995, 69-79.

Drucker, Peter. Managing in a Time of Great Change. New York: Truman Talley Books/Dutton, 1995.

Duggan, Richard. "Promoting Innovation in Industry, Government, and Higher Education." International Journal of Strategic Management, Vol. 29, No. 4, Aug, 1996, 503-513.

"Coca Clashes." The Economist,17 August 1996, 35-36.

"The Future of Warfare." The Economist, 8 March 1997, 15 and 21-24.

Executive Office of the President. A National Security Strategy for a New Century. Washington, D.C., May 1997.

Filippone, Robert. "The Medellín Cartel: Why We Can't Win the Drug War." Studies in Conflict and Terrorism, Vol. 17, No. 4, October 1994, 323-344.

French, Howard. "In Zaire's Eccentric War, Serbs Train Refugee Force." New York Times, 12 February 1997.

Fukuyama, Francis. "The end of History?" The National Interest, Summer 1989, 3-18.

Galbraith, Jay. Organization Design. Menlo Park, CA: Addison-Wesley Publishing Co., 1977, 36.

________. "The Innovating Organization." Organizational Dynamics, Winter 1982, 5-25.

Galbriath, Jay, Edward Lawler III, and Associates. Organizing for the Future. San Francisco: Jossey-Bass Publishers, 1993.

Gold, Phillip. "The New Frontier of Inter-Service Rivalry." Washington Times, 31 Aug 1994.

Gonzáles, Guadalupe, and Marta Tienda, eds. The Drug Connection in U.S.-Mexican Relations. San Diego: Center for U.S.-Mexican Studies, 1989, 48.

Graham, Bradley. "Battle Plans for a New Century." Washington Post, 21 Feb 1995.

Grandori, Anna, and Guiseppe Soda, "Inter-firm Networks: Antecedents, Mechanisms, and Forms." Organization Studies, 16/2, 1995, 183-214.

Hardy, Stephen. "Should We Fear the Byte Bomb?" Journal of Electronic Defense, Jan, 1996, 42-48.

Haeni, Reto E. and Lance J. Hoffman. An Introduction to Information Warfare. School of Engineering and Applied Sciences, George Washington University, Washington DC, Dec 1995.

Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. Command, Control, Communications and Computer Systems Directorate, Joint Staff, Washington DC. 4 Jul 1995.

"Information Warfare and Counterdrug Operations." Paper presented to the Directorate of Research, Air Command and Staff College, April 1996.

Jacob, Rahul. "The Struggle to Create an Organization." Fortune, 3 April 1995, 90-99.

James, Geoffrey. "Intranets Rescue Reengineering." Datamation, Vol. 42, No. 18, Dec 1996, 38-45.

Johnson, Stuart, and Martin Libicki, eds. Dominant Battlespace Knowledge: The Winning Edge. Washington DC: National Defense University Press, 1995.

Jones, David, (Gen). "Past Organizational Problems." Joint Forces Quarterly, Autumn 1996, 23-28.

Khandwalla, Pradip. The Design of Organizations. San Francisco: Harcourt Brace Jovanovich, Inc., 1977.

Keohane, Robert, and Joseph Nye. Power and Interdependence: World Politics in Transition. Boston: Little, Brown, 1977.

Kerry, John, (Sen). The New War: The Web of Crime That Threatens America's Security. New York: Simon and Schuster, 1997.

Kraus, George F., Jr., (CDR). "Information Warfare in 2015." Proceedings, Aug 1995, 42-45.

"Guerrilla Offensive Inflicts Big Losses." Latin American Weekly Report, 12 September 1996.

Lee, Rensselar, III. The White Labyrinth: Cocaine and Political Power. New Brunswick, NJ: Transaction Publishers, 1990.

Lemonick, Michael. "Animal Genocide, Mob Style." Time, 14 November 1994, 77-78.

Libicki, Martin. The Mesh and the Net. Institute for National Strategic Studies, National Defense University, Washington DC, 1994.

________. What is Information Warfare? Institute for National Strategic Studies, National Defense University, 1995.

Libicki, Martin, and James Halzett, "Do We Need an Information Corps?" Joint Forces Quarterly, Autumn 1993, 88-97.

MacDonald, Scott. Mountain High, White Avalanche. New York: Praeger, 1989.

Machiavelli, Niccolo. The Prince and The Discourses. New York: The Modern Library, 1940.

Marbry, Donald J., ed. The Latin American Narcotics Trade and U.S. National Security. New York: Greenwood Press, 1989.

March, James, and Johan Olsen. Ambiguity and Choice in Organizations. Bergen, Norway: Universitetsforlaget, 1979.

March, James, and Herbert Simon. Organizations. New York: John Wiley & Sons, Inc., 1958.

Markoff, John. "Cellular Industry Rejects U.S. Plan for Surveillance." New York Times, 20 September 1996.

________. "Code Set Up to Shield Privacy of Cellular Calls is Breached." New York Times, 20 March 1997.

Mason, John. "Russian 'in $2.8m Citibank computer fraud.'" Financial Times, 18 August 1995.

Maze, Rick. "Few Threats are Predicted." Air Force Times, 17 February 1997.

Mercer, Pamela. "Rebels Kill 80 in Strongest Attacks in Colombia in Decades." New York Times, 2 September 1996.

Mohrman, Allan, Jr., Susan Mohrman, Gerald Ledford, Jr., Thomas Cummings, Edward Lawler, III, and Associates. Large-Scale Organizational Change. San Francisco: Jossey-Bass Publishers, 1989.

Morgan, Gareth. Creative Organization Theory: A Resourcebook. Newbury Park, CA: SAGE Publications, 1989.

Munro, Neil. "The Pentagon's New Nightmare: An Electronic Pearl Harbor." The Washington Post, 16 July 1995, .

Murray, Williamson. "Innovation: Past and Future." Joint Forces Quarterly, Summer 1996, 51-60.

Negroponte, Nicholas. Being Digital. New York: Vintage Books, 1995.

Newman, Richard. "Warfare 2020." U.S. News & World Report, 5 August 1996, 34-42.

O'Connor, Anne-Marie. "U.S. Fears Escalation of Mexico's Drug Violence." The Los Angeles Times, 22 September 1996.

"Colombia Arrests Senator on Drug Corruption Charges." Orlando Sentinel, 25 April 1996.

Owens, William, (Adm), and Joseph Nye, Jr. "America's Information Edge." Foreign Affairs, March/April 1996, 20-36.

Perrow, Charles. Complex Organizations: A Critical Essay. Glenview, Ill.: Scott, Foresman, and Co., 1972.

Plato. The Republic. Translated by Francis Macdonald Cornford, Oxford: Oxford University Press, 1945.

Pohl, Frederik. The Cool War. New York : Ballantine Books, 1979.

Posen, Barry. The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars. Ithaca, NY: Cornell University Press, 1984.

Prager, Karsten. "Drugs, Money and a President's Ruin." Time, 5 February 1996, 37.

Pugh, Derek, and David Hickson. Writers on Organizations. Newbury Park, CA: SAGE Publications, 1989.

Quittner, Joshua. "From god@heaven.org: The Web is 'Anonymous.'" Time, 2 September, 1996, 57.

"U.S. Says Drug Smugglers Tried to Buy Sub," Reuters News Service, 7 February 1997.

Riley, Kevin Jack. The Implications of Colombian Drug Industry and Death Squad Political Violence for U.S. Counternarcotics Policy. N-3605-USDP, RAND report, Santa Monica, CA: RAND, 1993.

Robbins, Stephen. Organization Theory: Structure, Design, and Applications, 2nd ed. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1990, 312.

Robinson, Clarence. "Army Information Operations Protect Command and Control." Signal, July, 1996, 47-50.

________. "Rapid Technology Growth Spawns Land Information Warfare Activity." Signal, July, 1996, 51-54.

Rosen, Stephen. Winning the Next War: Innovation and the Modern Military. Ithaca, NY: Cornell University Press, 1991.

Rothberg, Robert. "They Slip Out of Nigeria and Drug the World." Christian Science Monitor, 24 September 1996, 19.

"Police Discover Cali Cartel Operations Inside Picota Jail." Santa Fe de Bogota Inravision Television, 10 December 1996.

Schnaubelt, Christopher. "Interagency Command and Control: Planning for Counterdrug Support," Military Review, September-October 1996, 16-24.

Schrieberg, David. "Birth of the Baby Cartels." Newsweek, 21 August 1995, 37.

Schwartau, Winn. Information Warfare. New York: Thunder's Mouth Press, 1994.

Schwartz, Peter. The Art of the Long View: Planning for the Future in an Uncertain World. New York: Doubleday, 1996

Scott, Peter, and Johnathan Marshall. Cocaine Politics. Berkeley: University of California Press, 1991.

Shalikashvili, John, (Gen). "A Word From the Chairman." Joint Forces Quarterly, Autumn 1996, 1.

Shannon, Elaine. "Reach Out and Waste Someone," Time Digital, July/August 1997, 35-39.

Shelton, Henry, (Gen). "Special Operations Forces: Looking Ahead." Defense '97, Issue 3, 32-41.

Simon, Herbert. Models of Bounded Rationality. Cambridge, Mass: MIT Press, 1982.

Slatalla, Michelle, and Joshua Quittner. Masters of Deception: The Gang That Ruled Cyberspace. New York: Harper Collins Publishers, 1995.

Slevin, Peter. "House Panel Wants Mexico Decertified." Miami Herald, 7 March 97.

Smith, Peter, ed. Drug Policy in the Americas. San Francisco: Westview Press, 1992.

Snow, Anita. "U.S. Lauds Colombia, Mexico for Drug-War Efforts." The Fresno Bee, 24 April 1996.

Stares, Paul. Global Habit: The Drug Problem in a Borderless World. Washington, DC: The Brookings Institution, 1996.

Sterling, Harry. "Mexican Bloodshed Reveals New Crisis, Drug Anarchy Could Follow Weakening of PRI's Iron Control." The Toronto Star, 7 October 1994.

Stohl, Clifford. The Cuckoo's Egg. New York: Simon & Schuster, 1989.

Strategic Information Warfare: A New Face of War. National Defense Research Institute, Santa Monica: RAND, 1996.

Sullivan, Gordon (Gen), and James Dubik (Col). War in the Information Age. Strategic Studies Institute, U.S. Army War College, 1994.

Szafranski, Richard (Col). A Theory of Information Warfare. Air University, Internet: www.cdsar.af.mil.

Toffler, Alvin. The Third Wave. New York: Bantam Books, 1980.

Toffler, Alvin, and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. New York: Little Brown and Co., 1993.

Tzu, Sun. The Art of War. Edited by James Clavel. New York: Dell Publishing, 1983, 2.

"USAF Opens First Information Warfare Training Laboratory." Internet: www.infowar.com/mil_c4I/mil_c4io.html-ssi.

U.S. Congress. House. Subcommittee on National Security, International Affairs, and Criminal Justice. Testimony of General Harold Bedoya Pizarro, General Commander of Colombian Military Forces, 14 February 1997.

U.S. Department of Defense. Joint Pub 3-07.4, Joint Counterdrug Operations. Washington DC, August 1994.

U.S. Department of Defense. Joint Pub 5-0, Doctrine for Planning Joint Operations. Washington DC, 13 April 1995.

U.S. Department of Justice. Drugs, Crime, and the Justice System. December 1992, 42.

U.S. Drug Enforcement Administration. Congressional Testimony. Drug Trafficking in Mexico. 28 March 1996.

U.S. Drug Enforcement Administration. Congressional Testimony. National Drug Control Strategy and Drug Interdiction. 12 September 1996.

U.S. Drug Enforcement Administration. Congressional Testimony. The Threat of Heroin to the United States. 19 September 1996.

U.S. Drug Enforcement Administration. Congressional Testimony. Mexico and the Southwest Border Initiative. 25 February 1997.

U.S. Drug Enforcement Administration Intelligence Bulletin. The South American Cocaine Trade: An Industry in Transition. 1 July 1996, 3.

U.S. Government Accounting Office. Drug Control: Counternarcotics Efforts in Mexico. GAO/NSIAD-96-163, June 1996, 3.

U.S. Office of National Drug Control Policy. Executive Office of the President. *1997 National Drug Control Strategy*. Washington DC, February 1997.

Waller, Douglas. "Onward Cyber Soldiers." Time, 21 August 1995, 38-48.

Watkins, Steven. "New Era has Humble Start." Air Force Times, 20 November 1995.

Weber, Max. The Theory of Social and Economic Organization. Translated by A. M. Henderson and Talcott Parsons. Edited by Talcott Parsons. New York: Free Press, 1947.

________. From Max Weber: Essays in Sociology. Translated and edited by Hans Gerth and C. Wright Mills. Oxford, UK: Oxford University Press, Inc., 1946.

Wilkinson, Tracy. "Safe in Cyberspace, Serbian Protests Flourish on the Net." LA Times, 8 December 1996.

Williamson, Oliver. Markets and Hierarchies: Analysis and Antitrust Implications. New York: Free Press, 1975.

Wilson, Catherine. "Two Accused in Nuke Sale Sting." Associated Press, 30 June 1997.

INITIAL DISTRIBUTION LIST

No. of copies

1. Defense Technical Information Center 2
8725 John J. Kingman R., STE 0944
Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
Naval Postgraduate School
411 Dyer Rd.
Monterey, CA 93943-5101

3. CAPT Frank C. Petho, Chairman 1
Department of National Security Affairs
Naval Postgraduate School
Monterey, CA 93943-5100

4. Associate Professor Daniel Moran, Code NS/MD 1
Academic Associate, Area Studies Curriculum
Naval Postgraduate School
Monterey, CA 93943-5100

5. Prof. John Arquilla, Code IW/AR 1
Naval Postgraduate School
Monterey, CA 93943-5100

6. Prof. Scott D. Tollefson, Code NS/TO 1
Naval Postgraduate School
Monterey, CA 93943-5100

7. Prof. Tom Bruneau, Code NS/BN 1
Naval Postgraduate School
Monterey, CA 93943-5100

8. Prof. Nancy Roberts, Code SM/RC 1
Naval Postgraduate School
Monterey, CA 93943-5100

9. Office of Secretary of Defense 1
Director, International Security Affairs
Inter-American Region
The Pentagon, Room 4C800
Washington, DC 20301

10. Office of Chief of Naval Operations 1
Western Hemisphere Branch
Political-Military Policy and Current Plans Division (N523)
The Pentagon, Room 4E519
Washington, DC 20350

11. Mr. Martin Scheina 1
Defense Intelligence Agency, Building 6000
Attention: PAW-4
Washington, DC 20340-3342

12. CAPT Richard O'Neill 1
Office of Assistant Secretary of Defense, C3I/Information Warfare
The Pentagon, Room 3D200
Washington, DC 20301-6000

13. Capt Alex Berger 1
Canaan Street, Box 65
Canaan, NH 03741